NISTIR 7628 Assessment Guide Companion Spreadsheet
CSWG-TC-001

The "Assessment Objectives worksheet contains the information to perform an assessment against the NISTIR 7628 high-level security requirements.

1) This worksheet is formatted to print on legal size paper.

2) The columns "Smart Grid Cyber Security Requirement", Req. Type", and "NISTIR 7628 Requirements Detail" are copied directly from the NISTIR 7628 (August 2010) high-level security requirements.

3) The columns "Assessment Objective", "Assessment Method", and "Potential Assessment Object(s)" are based on NIST SP800-53a then customizes to the NISTIR 7628 (August 2010) high-level security requirements.

4) The columns "Assessment Method" and "Potential Assessment Object(s)" can be customized to match the environment that is being assessed.

The "Assessment Method Definitions" worksheet is copied directly from NIST SP800-53a. This is a protected worksheet

The "NISTIR 7628 Mappings" worksheet is copied directly from a NISTIR 7628 August 2010 table. This is a protected worksheet.

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
			Access Control (SG.AC)			
SG.AC-1	Access Control Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented access control security policy that addresses— i. The objectives, roles, and responsibilities for the access control security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the access control security program as it applies to all of the organizational staff, contractors, and third parties. b. Procedures to address the implementation of the access control security policy and associated access control protection requirements. 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the access control security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The access control policy can be included as part of the general information security policy for the organization. Access control procedures can be developed for the security program in general and for a particular Smart Grid information system when required. Requirement Enhancements None. Additional Considerations None.	SG.AC-1.1 Determine if: (i) the organization develops and implements a documented access control policy; (ii) the access control policy addresses access control as it related to protecting the organization's personnel and assets and the following: a) purpose / objective b) scope c) roles and responsibilities e) coordination among organizational entities, and compliance; (iii) the access control policy addresses the scope to include all organizational staff, contractors, and third parties; (iv) the organization develops and implements the access control procedures; (v) the organization reviews and updates the access control procedures; (vi) management commitment ensures compliance with the organization's access control; (vii) the access control policy comply with applicable federal, state, local, tribal, and territorial laws and regulations; and (viii) the access control procedures facilitate implementation of the access control security policy. SG.AC-1.2 Determine if: (i) the organization defines the frequency of access control policy and procedures reviews/updates; (ii) the organization reviews/updates the access control policy and procedures in accordance with the organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.AC-2	Remote Access Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Documents allowed methods of remote access to the Smart Grid information system; 2. Establishes usage restrictions and implementation guidance for each allowed remote access method; 3. Authorizes remote access to the Smart Grid information system prior to connection; and 4. Enforces requirements for remote connections to the Smart Grid information system. Supplemental Guidance Remote access is any access to an organizational Smart Grid information system by a user (or process acting on behalf of a user) communicating through an external, non-organization-controlled network (e.g., the Internet). Requirement Enhancements None. Additional Considerations None.	SG.AC-2.1 Determine if: (i) the organization defines the situations and compelling operational needs when remote access to privileged functions on the Smart Grid information system is allowed; (ii) the organization documents the allowed remote access to the Smart Grid information system; (iii) the organization authorizes remote access to the Smart Grid information system prior to connection; (iv) the organization enforces requirements for remote connections to Smart Grid information systems. SG.AC-2.2 Determine if: (i) the organization defines managed access control points for remote access to the Smart Grid information system; and (ii) the Smart Grid information system controls all remote accesses through a limited number of managed access control points.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AC-3	Account Management	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization manages Smart Grid information system accounts, including: Authorizing, establishing, activating, modifying, disabling, and removing accounts; 1. Specifying account types, access rights, and privileges (e.g., individual, group, system, guest, anonymous and temporary); 2. Reviewing accounts on an organization-defined frequency; and 3. Notifying account managers when Smart Grid information system users are terminated, transferred, or Smart Grid information system usage changes. Management approval is required prior to establishing accounts. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization reviews currently active Smart Grid information system accounts on an organization-defined frequency to verify that temporary accounts and accounts of terminated or transferred users have been deactivated in accordance with organizational policy. A2. The organization authorizes and monitors the use of guest/anonymous accounts. A3. The organization employs automated mechanisms to support the management of Smart Grid information system accounts. A4. The Smart Grid information system automatically terminates temporary and emergency accounts after an organization-defined time period for each type of account. A5. The Smart Grid information system automatically disables inactive accounts after an organization-defined time period. A6. The Smart Grid information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	SG.AC-3.1 Determine if: (i) the organization manages Smart Grid information system accounts, including a) authorizing b) establishing c) activating d) modifying e) reviewing f) disabling g) removing accounts; (ii) the organization requires management approval prior to establishing accounts; (iii) the organization documents management approval prior to establishing accounts; (iv) the organization documents account types; (v) the organization documents access rights; (vi) the organization documents privileges. SG.AC-3.2 Determine if the organization reviews accounts in accordance with the organization-defined frequency. SG.AC-3.3 Determine if: (i) the organizations notified account managers when Smart Grid information system users are terminated; (ii) the organizations notified account managers when Smart Grid information system users are transferred; (iii) the organizations notified account managers when Smart Grid information system usage changes.	Examine, Interview, Test	Examine: [SELECT FROM: Access control policy; procedures addressing account management; standards and procedures on roles and responsibilities; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled Smart Grid information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with access control and remote access responsibilities]. Test: [SELECT FROM: emails, help desk ticket, remote access and access control requests, Smart Grid information systems containing accounts with remote access, monitoring reports, automated mechanisms implementing account management functions].
SG.AC-4	Access Enforcement	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The Smart Grid information system enforces assigned authorizations for controlling access to the Smart Grid information system in accordance with organization-defined policy. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization considers the implementation of a controlled, audited, and manual override of automated mechanisms in the event of emergencies.	SG.AC-4.1 Determine if the Smart Grid information system enforces assigned authorizations for controlling access to the system in accordance with the organizational defined policy.	Examine, Interview, Test	Examine: [SELECT FROM: Access control policy; procedures addressing account management; standards and procedures on roles and responsibilities; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled Smart Grid information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with access control and remote access responsibilities]. Test: [SELECT FROM: emails, help desk ticket, remote access and access control requests, Smart Grid information systems containing accounts with remote access, monitoring reports, automated mechanisms implementing account management functions].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AC-5	Information Flow Enforcement	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system enforces assigned authorizations for controlling the flow of information within the Smart Grid information system and between interconnected Smart Grid information systems in accordance with applicable policy. Supplemental Guidance Information flow control regulates where information is allowed to travel within a Smart Grid information system and between Smart Grid information systems. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict Smart Grid information system services or provide a packet-filtering capability. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system enforces information flow control using explicit labels on information, source, and destination objects as a basis for flow control decisions. A2. The Smart Grid information system enforces dynamic information flow control allowing or disallowing information flows based on changing conditions or operational considerations. A3. The Smart Grid information system enforces information flow control using organization-defined security policy filters as a basis for flow control decisions. A4. The Smart Grid information system enforces the use of human review for organization-defined security policy filters when the Smart Grid information system is not capable of making an information flow control decision. A5. The Smart Grid information system provides the capability for a privileged administrator to configure, enable, and disable the organization-defined security policy filters.	SG.AC-5.1 Determine if: (i) the Smart Grid information system enforces assigned authorizations for controlling the flow of information within the Smart Grid information system in accordance with the organizational policy; (ii) the Smart Grid information system enforces assigned authorizations for controlling the flow of information between interconnected systems in accordance with the organizational policy.	Examine, Interview, Test	Examine: [SELECT FROM: Access control policy; procedures addressing account management; standards and procedures on roles and responsibilities; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled Smart Grid information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with access control and remote access responsibilities]. Test: [SELECT FROM: emails, help desk ticket, remote access and access control requests, Smart Grid information systems containing accounts with remote access, monitoring reports, automated mechanisms implementing account management functions].
SG.AC-6	Separation of Duties	Tech	Category: Common Technical Requirements, Integrity Requirement The organization— 1. Establishes and documents divisions of responsibility and separates functions as needed to eliminate conflicts of interest and to ensure independence in the responsibilities and functions of individuals/roles; 2. Enforces separation of Smart Grid information system functions through assigned access authorizations; and 3. Restricts security functions to the least amount of users necessary to ensure the security of the Smart Grid information system. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations None.	SG.AC-6.1 Determine if: (i) the organization establishes divisions of responsibility as needed to eliminate conflicts of interest in the responsibilities and duties of individuals; (ii) the organization documents divisions of responsibility duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals; (iii) the organization establishes separation of duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals; (iv) the organization documents separation of duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals. SG.AC-6.2 Determine if the organization enforces separation of smart grid functions through assigned access authorizations. SG.AC-6.3 Determine if the organization restricts security functions to an organizational defined minimum amount of users necessary to ensure the security of the Smart Grid information system.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing account management; standards and procedures on roles and responsibilities; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled Smart Grid information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records]. Test: [SELECT FROM: emails, help desk ticket, remote access and access control requests, Smart Grid information systems containing accounts with remote access, monitoring reports, automated mechanisms implementing account management functions].
SG.AC-7	Least Privilege	Tech	Category: Common Technical Requirements, Integrity Requirement 1. The organization assigns the most restrictive set of rights and privileges or access needed by users for the performance of specified tasks; and 2. The organization configures the Smart Grid information system to enforce the most restrictive set of rights and privileges or access needed by users. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization authorizes network access to organization-defined privileged commands only for compelling operational needs and documents the rationale for such access in the security plan for the Smart Grid information system. A2. The organization authorizes access to organization-defined list of security functions (deployed in hardware, software, and firmware) and security-relevant information.	SG.AC-7.1 Determine if the organization assigns the most restrictive set of rights/privileges or accesses needed by users for the performance of specified tasks. SG.AC-7.2 Determine if the organization configures the Smart Grid information system to enforce the most restrictive set of rights/privileges or accesses needed by users.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing account management; standards and procedures on roles and responsibilities; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled Smart Grid information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records]. Test: [SELECT FROM: emails, help desk ticket, remote access and access control requests, Smart Grid information systems containing accounts with remote access, monitoring reports, automated mechanisms implementing account management functions].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AC-8	Unsuccessful Login Attempts	Tech	Category: Common Technical Requirements, Integrity Requirement The Smart Grid information system enforces a limit of organization-defined number of consecutive invalid login attempts by a user during an organization-defined time period. Supplemental Guidance Because of the potential for denial of service, automatic lockouts initiated by the Smart Grid information system are usually temporary and automatically released after a predetermined time period established by the organization. Permanent automatic lockouts initiated by a Smart Grid information system must be carefully considered before being used because of safety considerations and the potential for denial of service. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded; and A2. If a Smart Grid information system cannot perform account/node locking or delayed logins because of significant adverse impact on performance, safety, or reliability, the system employs alternative requirements or countermeasures that include the following: c. Real-time logging and recording of unsuccessful login attempts; and d. Real-time alerting of a management authority for the Smart Grid information system when the number of defined consecutive invalid access attempts is exceeded.	SG.AC-8.1 Determine if: (i) the organization defines a limit of consecutive invalid access attempts by a user during an organization-defined time period; (ii) the organization enforces the limit of consecutive invalid access attempts by a user during an organization-defined time period; (iii) the organization defines the time period for consecutive invalid access attempts by a user.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing account management; standards and procedures on roles and responsibilities; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled Smart Grid information system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records]. Test: [SELECT FROM: emails, help desk ticket, remote access and access control requests, Smart Grid information systems containing accounts with remote access, monitoring reports, automated mechanisms implementing account management functions].
SG.AC-9	Smart Grid Information System Use Notification	Tech	Category: Common Technical Requirements, Integrity Requirement The Smart Grid information system displays an approved system use notification message or banner before granting access to the Smart Grid information system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance. Supplemental Guidance Smart Grid information system use notification messages can be implemented in the form of warning banners displayed when individuals log in to the Smart Grid information system. Smart Grid information system use notification is intended only for Smart Grid information system access that includes an interactive interface with a human user and is not intended to call for such an interface when the interface does not currently exist. Requirement Enhancements None. Additional Considerations None.	SG.AC-9.1 Determine if: (i) the organization defines a system use notification message / banner for security and privacy for the Smart Grid information system consistent with applicable laws, directives, policies, regulations, standards, and guidance; (ii) the organization documents a system use notification message / banner for security and privacy for the Smart Grid information system; (iii) the organization approves a system use notification message /banner for security and privacy for the Smart Grid information system; (iv) the Smart Grid information system displays an approved system use notification message / banner for security and privacy before granting Smart Grid information system access.	Examine, Test	Examine: [SELECT FROM: Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of Smart Grid information system use notification messages or banners; Smart Grid information system notification messages; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records for user acceptance of notification message or banner; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing the access control policy for system use notification].
SG.AC-10	Previous Logon Notification	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system notifies the user, upon successful logon, of the date and time of the last logon and the number of unsuccessful logon attempts since the last successful logon. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations None.	SG.AC-10.1 Determine if: (i) the Smart Grid information system, upon successful logon, displays a) the date of the last logon; b) the time of the last logon; c) the number of unsuccessful logon attempts since the last successful logon.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing previous logon notification; Smart Grid information system configuration settings and associated documentation; Smart Grid information system notification messages; Smart Grid information system design documentation; Smart Grid information system design documentation; Smart Grid information system audit records; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing the access control policy for previous logon notification].
SG.AC-11	Concurrent Session Control	Tech	Category: Unique Technical Requirements Requirement The organization limits the number of concurrent sessions for any user on the Smart Grid information system. Supplemental Guidance The organization may define the maximum number of concurrent sessions for a Smart Grid information system account globally, by account type, by account, or a combination. This requirement addresses concurrent sessions for a given Smart Grid information system account and does not address concurrent sessions by a single user via multiple Smart Grid information system accounts. Requirement Enhancements None. Additional Considerations None.	SG.AC-11.1 Determine if: (i) the organization defines the limit of concurrent sessions for any user on the Smart Grid information system; (ii) the organization enforces the limit of concurrent sessions for any user on the Smart Grid information system.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing previous logon notification; Smart Grid information system configuration settings and associated documentation; Smart Grid information system notification messages; Smart Grid information system design documentation; Smart Grid information system design documentation; Smart Grid information system audit records; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing the access control policy for concurrent session control].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AC-12	Session Lock	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system— 1. Prevents further access to the Smart Grid information system by initiating a session lock after an organization-defined time period of inactivity or upon receiving a request from a user; and 2. Retains the session lock until the user reestablishes access using appropriate identification and authentication procedures. Supplemental Guidance A session lock is not a substitute for logging out of the Smart Grid information system. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system session lock mechanism, when activated on a device with a display screen, places a publicly viewable pattern onto the associated display, hiding what was previously visible on the screen.	SG.AC-12.1 Determine if: (i) the organization defines the time period of user inactivity after which the Smart Grid information system initiates a session lock; (ii) the organization enforces the time period of user inactivity after which the Smart Grid information system initiates a session lock of receiving a request from a user. SG.AC-12.2 Determine if the Smart Grid information system maintains the session lock until the user reestablishes access using appropriate identification and authentication procedures.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing session lock; display screen with session lock activated; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; security plan; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing the access control policy for session lock; Smart Grid information system session lock mechanisms].
SG.AC-13	Remote Session Termination	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system terminates a remote session at the end of the session or after an organization-defined time period of inactivity. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. Automatic session termination applies to local and remote sessions.	SG.AC-13.1 Determine if: (i) the organization defines the time period of remote user inactivity after which the Smart Grid information system initiates a session lock; (ii) the organization enforces the time period of remote user inactivity after which the Smart Grid information system initiates a session lock of receiving a request from a user; (iii) the Smart Grid information system terminates a remote session at the end of the remote session or after the organizationally defined remote access inactivity period.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing session timing and termination; display screen with session lock activated; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; security plan; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing the access control policy for session lock; Smart Grid information system session timing and termination mechanisms].
SG.AC-14	Permitted Actions without Identification or Authentication	Tech	Category: Unique Technical Requirements Requirement 1. The organization identifies and documents specific user actions, if any, that can be performed on the Smart Grid information system without identification or authentication; and 2. Organizations identify any actions that normally require identification or authentication but may, under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. Supplemental Guidance The organization may allow limited user actions without identification and authentication (e.g., when individuals access public Web sites or other publicly accessible Smart Grid information systems. Requirement Enhancements 3. The organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives. Additional Considerations None.	SG.AC-14.1 Determine if: (i) the organization identifies specific user actions that can be performed on the Smart Grid information system without identification or authentication; (ii) the organization documents specific user actions that can be performed on the Smart Grid information system without identification or authentication. SG.AC-14.2 Determine if the organization identifies any actions that normally require identification or authentication but may, under certain circumstances (e.g., emergencies), allow identification or authentication mechanisms to be bypassed. SG.AC-14.3 Determine if the organization permits actions to be performed without identification and authentication only to the extent necessary to accomplish mission objectives.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing permitted actions without identification and authentication; Smart Grid information system configuration settings and associated documentation; security plan; list of Smart Grid information system actions that can be performed without identification and authentication; Smart Grid information system audit records; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing the access control policy for sessions without identity or with unauthenticated access; Smart Grid information system session lock mechanisms].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AC-15	Remote Access	Tech	Category: Unique Technical Requirements Requirement The organization authorizes, monitors, and manages all methods of remote access to the Smart Grid information system. Supplemental Guidance Remote access is any access to a Smart Grid information system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet). Requirement Enhancements 1. The organization authenticates remote access, and uses cryptography to protect the confidentiality and integrity of remote access sessions; 2. The Smart Grid information system routes all remote accesses through a limited number of managed access control points; 3. The Smart Grid information system protects wireless access to the Smart Grid information system using authentication and encryption. Note: Authentication applies to user, device, or both as necessary; and 4. The organization monitors for unauthorized remote connections to the Smart Grid information system, including scanning for unauthorized wireless access points on an organization-defined frequency and takes appropriate action if an unauthorized connection is discovered. Additional Considerations A1. Remote access to Smart Grid information system component locations (e.g., control center, field locations) is enabled only when necessary, approved, authenticated, and for the duration necessary; A2. The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods; A3. The organization authorizes remote access for privileged commands and security-relevant information only for compelling operational needs and documents the rationale for such access in the security plan for the Smart Grid information system; and A4. The organization disables, when not intended for use, wireless networking capabilities internally embedded within Smart Grid information system components.	SG.AC-15.1 Determine if: (i) the organization authorizes remote access to the Smart Grid information system for all allowed methods of remote access; (ii) the organization monitors remote access to the Smart Grid information system for all allowed methods of remote access; (iii) the organization controls remote access to the Smart Grid information system for all allowed methods of remote access. SG.AC-15.2 Determine if: (i) the organization authenticates remote access; (ii) the organization uses cryptography to protect the confidentiality and integrity of remote access sessions; SG.AC-15.3 Determine if: (i) the organization defines a limited number of managed access control points for remote access to the Smart Grid information system; and (ii) the Smart Grid information system controls all remote accesses through a limited number of managed access control points. SG.AC-15.4 Determine if: (i) the organization defines the protection of wireless access to the Smart Grid information system by using authentication and encryption; (ii) the Smart Grid information system uses authentication and encryption to protect wireless access. SG.AC-15.5 Determine if: (i) the organization monitors for unauthorized remote connections to the Smart Grid information system and takes appropriate action if an unauthorized connection is discovered; (ii) the organization defines a frequency for scanning wireless access points; (iii) the organization defines actions for unauthorized wireless connections to the Smart Grid information system; (iv) the organization enforces the actions for unauthorized wireless connections to the Smart Grid information system.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing remote access to the Smart Grid information system; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; security plan; list of networking protocols deemed to be not secure; other relevant documents or records]. Test: [SELECT FROM: Remote access methods for the Smart Grid information system; Automated mechanisms implementing the access control policy for remote access; Automated mechanisms disabling networking protocols deemed to be not secure].
SG.AC-16	Wireless Access Restrictions	Tech	Category: Common Technical Requirements, Confidentiality Requirement The organization— 1. Establishes use restrictions and implementation guidance for wireless technologies; and 2. Authorizes, monitors, and manages wireless access to the Smart Grid information system. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization uses authentication and encryption to protect wireless access to the Smart Grid information system; and A2. The organization scans for unauthorized wireless access points at an organization-defined frequency and takes appropriate action if such access points are discovered.	SG.AC-16.1 Determine if: (i) the organization establishes use restrictions and implementation guidance for wireless technologies; (ii) the organization authorizes wireless access to the Smart Grid information system; (iii) the organization monitors wireless access to the Smart Grid information system; (iv) the organization manages wireless access to the Smart Grid information system.	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing remote access to the Smart Grid information system; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; security plan; list of networking protocols deemed to be not secure; policy and procedures addressing wireless access and wireless access points; other relevant documents or records]. Test: [SELECT FROM: Remote access methods for the Smart Grid information system; Automated mechanisms implementing the access control policy for remote access; Automated mechanisms disabling networking protocols deemed to be not secure; wireless scanning assessments].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AC-17	Access Control for Portable and Mobile Devices	Tech	Category: Common Technical Requirements, Confidentiality Requirement The organization— 1. Establishes usage restrictions and implementation guidance for organization-controlled mobile devices, including the use of writeable, removable media and personally owned removable media; 2. Authorizes connection of mobile devices to Smart Grid information systems; 3. Monitors for unauthorized connections of mobile devices to Smart Grid information systems; and 4. Enforces requirements for the connection of mobile devices to Smart Grid information systems. Supplemental Guidance Specially configured mobile devices include computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel to locations that the organization determines to be of significant risk, include examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Requirement Enhancements The organization— 1. Controls the use of writable, removable media in Smart Grid information systems; 2. Controls the use of personally owned, removable media in Smart Grid information systems; 3. Issues specially configured mobile devices to individuals traveling to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures; and 4. Applies specified measures to mobile devices returning from locations that the organization determines to be of significant risk in accordance with organizational policies and procedures. Additional Considerations None.	SG.AC-17.1 Determine if: (i) the organization establishes usage restrictions for organization-controlled portable and mobile devices, including the use of writeable, removable media and personally owned removable media; (ii) the organization establishes implementation guidance for organization-controlled portable and mobile devices, including the use of writeable, removable media and personally owned removable media. SG.AC-17.2 Determine if the organization authorizes connections of mobile devices to the Smart Grid information system. SG.AC-17.3 Determine if the organization monitors for unauthorized connections of mobile devices to the Smart Grid information system. SG.AC-17.4 Determine if: (i) the organization documents requirements for the connection of mobile devices to the Smart Grid information system; (ii) the organization enforces requirements for the connection of mobile devices to the Smart Grid information system. SG.AC-17.5 Determine if: (i) the organization documents the use of writable, removable media in Smart Grid information systems; (ii) the organizations controls the use of writable, removable media in Smart Grid information systems. SG.AC-17.6 Determine if: (i) the organization documents the use of personally owned removable media in Smart Grid information systems; (ii) the organizations controls the use personally owned removable media in Smart Grid information systems. SG.AC-17.7 Determine if: (i) the organization documents the configuration of mobile devices assigned to individual travelling to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures; (ii) the organization maintains the organizationally defined configured mobile devices to be assigned to individual travelling to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures; (iii) the organization provides organizationally defined configured mobile devices to be assigned to individual travel to locations that the organization determines to be of significant risk in accordance with organizational policies and procedures. SG.AC-17.8 Determine if:	Examine, Test	Examine: [SELECT FROM: Access control policy; procedures addressing access control for portable and mobile devices; evidentiary documentation for random inspections of mobile devices; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing access control policy for portable and mobile devices; automated mechanisms prohibiting the use of internal or external modems or wireless interfaces with mobile devices].
SG.AC-18	Use of External Information Control Systems	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization establishes terms and conditions for authorized individuals to— 1. Access the Smart Grid information system from an external information system; and 2. Process, store, and transmit organization-controlled information using an external information system. Supplemental Guidance External information systems are information systems or components of information systems that are outside the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of security requirements or the assessment of security requirement effectiveness. Requirement Enhancements 1. The organization imposes restrictions on authorized individuals with regard to the use of organization-controlled removable media on external information systems. Additional Considerations A1. The organization prohibits authorized individuals from using an external information system to access the Smart Grid information system or to process, store, or transmit organization-controlled information except in situations where the organization (a) can verify the implementation of required security controls on the external information system as specified in the organization's security policy and security plan, or (b) has approved Smart Grid information system connection or processing agreements with the organizational entity hosting the external information system.	SG.AC-18.1 Determine if the organizations documents terms and conditions for authorized individual to access the Smart Grid information system from an external Smart Grid information system. SG.AC-18.2 Determine if the organizations documents terms and conditions for authorized individual to a) process organization-controlled information using an external Smart Grid information system; b) store organization-controlled information using an external Smart Grid information system; c) transmit organization-controlled information using an external Smart Grid information system. SG.AC-18.3 Determine if: (i) the organizations documents restrictions on authorized individual with regard to the use of organization-controlled removable media on external Smart Grid information systems; (ii) the organizations enforces restrictions on authorized individual with regard to the use of organization-controlled removable media on external Smart Grid information systems.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the Smart Grid information system; list of mediation vehicles for allowing public access to the organization's internal networks; Smart Grid information system design documentation; boundary protection hardware and software; Smart Grid information system configuration settings and associated documentation; communications and network traffic monitoring logs; enterprise security architecture documentation; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing boundary protection capability within the Smart Grid information system; Automated mechanisms implementing access controls for public access to the organization's internal networks].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AC-19	Control System Access Restrictions	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization employs mechanisms in the design and implementation of a Smart Grid information system to restrict access to the Smart Grid information system from the organization's enterprise network. Supplemental Guidance Access to the Smart Grid information system to satisfy business requirements needs to be limited to read-only access. Requirement Enhancements None. Additional Considerations None.	SG.AC-19.1 Determine if: (i) the organization documents mechanisms in the design and implementation of a Smart Grid information system to restrict access to the Smart Grid information system from the organization's enterprise network; (ii) the organization implements mechanisms in the design and implementation of a Smart Grid information system to restrict access to the Smart Grid information system from the organization's enterprise network; (iii) the organization enforces mechanisms in the design and implementation of a Smart Grid information system to restrict access to the Smart Grid information system from the organization's enterprise network.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the Smart Grid information system; list of mediation vehicles for allowing public access to the organization's internal networks; Smart Grid information system design documentation; boundary protection hardware and software; Smart Grid information system configuration settings and associated documentation; communications and network traffic monitoring logs; enterprise security architecture documentation; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing boundary protection capability within the Smart Grid information system; Automated mechanisms implementing access controls for public access to the organization's internal networks].
SG.AC-20	Publicly Accessible Content	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Designates individuals authorized to post information onto an organizational information system that is publicly accessible; 2. Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information; 3. Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system; 4. Reviews the content on the publicly accessible organizational information system for nonpublic information on an organization-defined frequency; and 5. Removes nonpublic information from the publicly accessible organizational information system, if discovered. Supplemental Guidance Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information. This requirement addresses posting information on an organizational information system that is accessible to the general public, typically without identification or authentication. Requirement Enhancements None. Additional Considerations None.	SG.AC-20.1 Determine if the organization designates individuals authorized to post information onto an organizational Smart Grid information system that is publicly accessible. SG.AC-20.2 Determine if the organization trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information. SG.AC-20.3 Determine if the organization reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational Smart Grid information system. SG.AC-20.4 Determine if the organization reviews the content on the publicly accessible organizational Smart Grid information system for nonpublic information on an organization-defined frequency. SG.AC-20.5 Determine if the organization removes nonpublic information from the publicly accessible organizational Smart Grid information system, if discovered.	Examine, Interview	Examine: [SELECT FROM: Public information policy; Social media policy; procedures for posting publicly available information; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for posting and maintaining public content].
SG.AC-21	Passwords	Tech	Category: Common Technical Requirements, Integrity Requirement 1. The organization develops and enforces policies and procedures for Smart Grid information system users concerning the generation and use of passwords; 2. These policies stipulate rules of complexity, based on the criticality level of the Smart Grid information system to be accessed; and 3. Passwords shall be changed regularly and are revoked after an extended period of inactivity. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations None.	SG.AC-21.1 Determine if: (i) the organization develops policies and procedures for Smart Grid information system users concerning the generation and use of passwords; (ii) the organization implements policies and procedures for Smart Grid information system users concerning the generation and use of passwords; (iii) the organization enforces policies and procedures for Smart Grid information system users concerning the generation and use of passwords. SG.AC-21.2 Determine if the organizational policies document rules of complexity, based on the criticality level of the Smart Grid information system to be accessed. SG.AC-21.3 Determine if: (i) the organizational policies document rules of passwords shall be changed regularly; (ii) the organizational policies document rules of passwords shall be revoked after an extended period of inactivity.	Examine, Test	Examine: [SELECT FROM: Password policy; Authentication policy; procedures addressing authentication and password control; security plan; list of active system accounts along with the name of the individual associated with each account and the last time the password has been changed; list of guest / anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires and the last time the password was changed; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing password policy management; automated mechanisms for changing passwords; Automated mechanisms for password expiration].
Awareness and Training (SG.AT)						

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AT-1	Awareness and Training Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented awareness and training security policy that addresses— i. The objectives, roles, and responsibilities for the awareness and training security program as it relates to protecting the organization's personnel and assets, and ii. The scope of the awareness and training security program as it applies to all of the organizational staff, contractors, and third parties. b. Procedures to address the implementation of the awareness and training security policy and associated awareness and training protection requirements. 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the awareness and training security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The security awareness and training policy can be included as part of the general information security policy for the organization. Security awareness and training procedures can be developed for the security program in general and for a particular Smart Grid information system when required. Requirement Enhancements None. Additional Considerations None.	SG-AT-1.1 Determine if: (i) the organization develops and implements a documented security awareness and training policy; (ii) the security awareness and training policy addresses security awareness and training as it related to protecting the organization's personnel and assets and the following: a) purpose / objective b) scope c) roles and responsibilities d) coordination among organizational entities, and compliance; (iii) the security awareness and training policy addresses the scope to include all organizational staff, contractors, and third parties; (iv) the organization develops and implements the security awareness and training procedures; (v) the organization reviews and updates the security awareness and training procedures; (vi) management commitment ensures compliance with the organization's security awareness and training; (vii) the security awareness and training policy comply with applicable federal, state, local, tribal, and territorial laws and regulations; and (viii) the security awareness and training procedures facilitate implementation of the security awareness and training security policy. SG-AT-1.2 Determine if: (i) the organization defines the frequency of security awareness and training policy and procedures reviews/updates; (ii) the organization reviews/updates the security awareness and training policy and procedures in accordance with the organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.AT-2	Security Awareness	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization provides basic security awareness briefings to all Smart Grid information system users (including employees, contractors, and third parties) on an organization-defined frequency. Supplemental Guidance The organization determines the content of security awareness briefings based on the specific requirements of the organization and the Smart Grid information system to which personnel have authorized access. Requirement Enhancements None. Additional Considerations A1. All Smart Grid information system design and procedure changes need to be reviewed by the organization for inclusion in the organization security awareness training; and A2. The organization includes practical exercises in security awareness briefings that simulate actual cyber attacks.	SG.AT-2.1 Determine if: (i) the organization provides basic security awareness training to all Smart Grid information system users on an organizational defined frequency; (ii) the organization includes exercises during the security awareness briefings that similar cyber attacks; (iii) the scope of the policy and procedure include organization staff, contractors and third parties; (iv) the security awareness and training materials address the specific requirements of the organization and the Smart Grid information systems to which personnel have authorized access; (v) Smart Grid information system design changes are reviewed for inclusion in the organization awareness training; (vi) Smart Grid information system procedure changes are reviewed for inclusion in the organization awareness training.	Examine, Interview	Examine: [SELECT FROM: Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of federal regulations; security awareness training curriculum; security awareness training materials; security plan; training records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel comprising the general Smart Grid information system user community; Organizational personnel that participate in security awareness training].
SG.AT-3	Security Training	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization provides security-related training— 1. Before authorizing access to the Smart Grid information system or performing assigned duties; 2. When required by Smart Grid information system changes; and 3. On an organization-defined frequency thereafter. Supplemental Guidance The organization determines the content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the Smart Grid information system to which personnel have authorized access. In addition, the organization provides Smart Grid information system managers, Smart Grid information system and network administrators, and other personnel having access to Smart Grid information system-level software, security-related training to perform their assigned duties. Requirement Enhancements None. Additional Considerations	SG.AT-3.1 Determine if: (i) the organization provides security training before authorizing access to the Smart Grid information system; (ii) the organization provides security training before performing duties for accessing the Smart Grid information system; (iii) the organization provides security training when required by the Smart Grid information system; (iv) the organization provides security training on an organizational defined frequency; (v) the organization security training includes a) roles and responsibilities b) organizational requirements c) security-related training for assigned duties.	Examine, Interview	Examine: [SELECT FROM: Security awareness and training policy; procedures addressing security training implementation; codes of federal regulations; security training curriculum; security training materials; security plan; training records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for role-based, security-related training; organizational personnel with significant Smart Grid information system security responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AT-4	Security Awareness and Training Records	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization maintains a record of awareness and training for each user in accordance with the provisions of the organization's training and records retention policy. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations	SG.AT-4.1 Determine if: (i) the organization maintains training records for each user; (ii) the organization maintains training records in accordance with the organization records retention policy.	Examine, Interview	Examine: [SELECT FROM: Security awareness and training policy; procedures addressing security training records; security awareness and training records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security training record retention responsibilities].
SG.AT-5	Contact with Security Groups and Associations	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization establishes and maintains contact with security groups and associations to stay up to date with the latest recommended security practices, techniques, and technologies and to share current security-related information including threats, vulnerabilities, and incidents. Supplemental Guidance Security groups and associations can include special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. The groups and associations selected are consistent with the organization's mission/business requirements. Requirement Enhancements None. Additional Considerations	SG.AT-5.1 Determine if the organization (i) establishes contact with security group and associations; (ii) maintains contact with security group and associations; (iii) stays up to date on the latest recommended security practices, techniques, and technologies; and (iv) shares current security-related information including threats, vulnerabilities, and incidents.	Examine, Interview	Examine: [SELECT FROM: Security awareness and training policy; procedures addressing contacts with security groups and associations; list of organization-defined key contacts to obtain ongoing Smart Grid information system security knowledge, expertise, and general information; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security responsibilities (e.g., individuals that have contacts with selected groups and associations within the security community)].
SG.AT-6	Security Responsibility Training	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization tests the knowledge of personnel on security policies and procedures based on their roles and responsibilities to ensure that they understand their responsibilities in securing the Smart Grid information system; 2. The organization maintains a list of security responsibilities for roles that are used to test each user in accordance with the provisions of the organization training policy; and 3. The security responsibility testing needs to be conducted on an organization-defined frequency and as warranted by technology/procedural changes. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations None.	SG.AT-6.1 Determine if the organization (i) tests the knowledge of security policies and procedures to ensure knowledge of responsibilities; (ii) maintains a list of security responsibilities for each role; (iii) conducts security responsibility testing on an organizational defined frequency.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; Security training plan; procedures addressing security training plan development and implementation; procedures addressing security plan reviews and updates; other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with security training responsibilities for the Smart Grid information system].
SG.AT-7	Planning Process Training	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization includes training in the organization's planning process on the implementation of the Smart Grid information system security plans for employees, contractors, and third parties. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations	SG.AT-7.1 Determine if: (i) the organization security training includes the planning process on implementing Smart Grid information systems security plans; (ii) the organization security training includes organization staff, contractors and third parties.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; Security training plan; procedures addressing security training plan development and implementation; procedures addressing security plan reviews and updates; other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with security training responsibilities for the Smart Grid information system].
Audit and Accountability (SG.AU)						

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AU-1	Audit and Accountability	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented audit and accountability security policy that addresses— i. The objectives, roles, and responsibilities for the audit and accountability security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the audit and accountability security program as it applies to all of the organizational staff, contractors, and third parties. b. Procedures to address the implementation of the audit and accountability security policy and associated audit and accountability protection requirements. 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the audit and accountability security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The audit and accountability policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general and for a particular Smart Grid information system when required. Requirement Enhancements None.	SG-AU-1.1 Determine if: (i) the organization develops and implements a documented audit and accountability security policy; (ii) the audit and accountability security policy addresses the objectives, roles, responsibility and scope of the audit and accountability security program; (iii) the organization develops, implements, reviews and updates a audit and accountability procedures; (iv) management commitment ensures compliance with the organization's security; (v) the audit and accountability policy comply with applicable federal, state, local, tribal, and territorial laws and regulations; and (vi) the audit and accountability procedures facilitate implementation of the audit and accountability security policy. SG-AU-1.2 Determine if: (i) the organization defines the frequency of audit and accountability security policy reviews/updates; (ii) the organization reviews/updates the audit and accountability security policy in accordance with the organization-defined frequency; (iii) the organization defines the frequency of audit and accountability procedures reviews/updates; and (iv) the organization reviews/updates the audit and accountability procedures in accordance with the organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.AU-2	Auditable Events	Tech	Category: Common Technical Requirements, Integrity Requirement The organization— 1. Develops, based on a risk assessment, the Smart Grid information system list of auditable events on an organization-defined frequency; 2. Includes execution of privileged functions in the list of events to be audited by the Smart Grid information system; and 3. Revises the list of auditable events based on current threat data, assessment of risk, and post-incident analysis. Supplemental Guidance The purpose of this requirement is for the organization to identify events that need to be auditable as significant and relevant to the security of the Smart Grid information system. Requirement Enhancements 1. The organization should audit activities associated with configuration changes to the Smart Grid information system. Additional Considerations None.	SG.AU-2.1 Determine if: (i) the organization defines the list of events the Smart Grid information system must be capable of auditing based on a risk assessment; (ii) the organization-defined auditable events include execution of privileged functions; (iii) the Smart Grid information system generates audit records for the organization-defined auditable events; (iv) the organization specifies which Smart Grid information system components carry out auditing activities; and (v) the organization decides, based upon a risk assessment, which events require auditing on a continuous basis and which events require auditing in response to specific situations. SG.AU-2.2 Determine if: (i) the organization defines the frequency of revising the list of auditable events reviews/updates; and (ii) the organization revises the list of auditable events in accordance with the organization-defined frequency. SG.AU-2.3 (requirements enhancement 1) Determine if the organization audits activities associated with configuration changes to the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing auditable events; security plan; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; list of organization-defined auditable events; auditable events review and update records; Smart Grid information system incident reports; list of Smart Grid information system auditable events; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with auditing and accountability responsibilities; Organizational personnel with responsibilities for monitoring open source information for evidence of unauthorized exfiltration or disclosure].
SG.AU-3	Content of Audit Records	Tech	Category: Common Technical Requirements, Integrity Requirement The Smart Grid information system produces audit records for each event. The record contains the following information: • Data and time of the event, • The component of the Smart Grid information system where the event occurred, • Type of event, • User/subject identity, and • The outcome of the events. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system provides the capability to include additional, more detailed information in the audit records for audit events identified by type, location, or subject; and A2. The Smart Grid information system provides the capability to centrally manage the content of audit records generated by individual components throughout the Smart Grid information system.	SG.AU-3.1 Determine if: (i) all types of Smart Grid information system audit records record the date and time of the event; (ii) all types of Smart Grid information system audit records record the component where the event occurred; (iii) all types of Smart Grid information system audit records record the type of event; (iv) all types of Smart Grid information system audit records record the identity of the user/subject that caused the event; and (v) all types of Smart Grid information system audit records record the outcome of the event.	Examine, Interview, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; Smart Grid information system audit records; Smart Grid information system incident reports; Smart Grid information system design documentation; security plan; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with auditing and accountability responsibilities; Organizational personnel with responsibilities for monitoring open source information for evidence of unauthorized exfiltration or disclosure]. Test: [SELECT FROM: Automated mechanisms implementing Smart Grid information system auditing of auditable events; Smart Grid information system audit capability to include more detailed information in audit records for audit events identified by type, location, or subject].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AU-4	Audit Storage Capacity	Tech	Category: Common Technical Requirements, Integrity Requirement The organization allocates organization-defined audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded. Supplemental Guidance The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Requirement Enhancements None. Additional Considerations -	SG.AU-4.1 Determine if: (i) the organization defines the audit record storage capacity for all Smart Grid information systems; (ii) the organization allocates audit record storage capacity in accordance with the organization defined limits; and (iii) the organization configures auditing to reduce the likelihood of audit record storage capacity being exceeded.	Examine, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit storage capacity; Smart Grid information system design documentation; organization-defined audit record storage capacity for Smart Grid information system components that store audit records; list of organization-defined auditable events; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; other relevant documents or records]. Test: [SELECT FROM: Audit record storage capacity and related configuration settings].
SG.AU-5	Response to Audit Processing Failures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The Smart Grid information system— 1. Alerts designated organizational officials in the event of an audit processing failure; and 2. Executes an organization-defined set of actions to be taken (e.g., shutdown Smart Grid information system, overwrite oldest audit records, and stop generating audit records). Supplemental Guidance Audit processing failures include software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Requirement Enhancements 1. The Smart Grid information system provides a warning when allocated audit record storage volume reaches an organization-defined percentage of maximum audit record storage capacity; and 2. The Smart Grid information system provides a real-time alert for organization defined audit failure events. Additional Considerations	SG.AU-5.1 Determine if: (i) the organization designates the personnel to be notified in case of an audit processing failure; and (ii) the Smart Grid information system alerts designated organizational officials; (iii) the organization defines in the security plan actions to be taken in the event of an audit processing failure; and (iv) the Smart Grid information systems perform the organization-defined actions when audit processing failure occurs. SG.AU-5.2 (requirements enhancement 1) Determine if the Smart Grid information system provides a warning when allocated audit record storage volume reaches an organization-defined percentage of maximum audit record storage capacity. SG.AU-5.3 (requirements enhancement 2) Determine if: (i) the organization defines what audit failures result in a real-time alert; and (ii) the Smart Grid information system provides a real-time alert for those organization defined audit failure events.	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing response to audit processing failures; Smart Grid information system design documentation; security plan; Smart Grid information system configuration settings and associated documentation; list of personnel to be notified in case of an audit processing failure; Smart Grid information system audit records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with auditing and accountability responsibilities; Organizational personnel with responsibilities for monitoring open source information for evidence of unauthorized exfiltration or disclosure].
SG.AU-6	Audit Monitoring, Analysis, and Reporting	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Reviews and analyzes Smart Grid information system audit records on an organization-defined frequency for indications of inappropriate or unusual activity and reports findings to management authority; and 2. Adjusts the level of audit review, analysis, and reporting within the Smart Grid information system when a change in risk occurs to organizational operations, organizational assets, or individuals. Supplemental Guidance Organizations increase the level of audit monitoring and analysis activity within the Smart Grid information system based on, for example, law enforcement information, intelligence information, or other credible sources of information. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system employs automated mechanisms to integrate audit review, analysis, and reporting into organizational processes for investigation and response to suspicious activities; A2. The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness; A3. The Smart Grid information system employs automated mechanisms to centralize audit review and analysis of audit records from multiple components within the Smart Grid information system; and A4. The organization integrates analysis of audit records with analysis of performance and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.	SG.AU-6.1 Determine if: (i) the organization regularly reviews/analyzes audit records for indications of inappropriate or unusual activity; (ii) the organization investigates suspicious activity or suspected violations; (iii) the organization designates management authorities to whom findings of inappropriate or unusual activities are reported; and (iv) the organization reports findings of inappropriate/unusual activities, suspicious behavior, or suspected violations to the designated management authorities. SG.AU-6.2 Determine if organization adjusts the level of audit review, analysis, and reporting within the Smart Grid information system when a change in risk occurs due to organizational operations, organizational assets, or individuals.	Examine, Interview, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews / analyses of audit records; procedures for investigating and responding to suspicious activities; threat information documentation from law enforcement, intelligence community, or other sources; Smart Grid information system configuration settings and associated documentation; integrated analysis of audit records, vulnerability scanning information, performance data, network monitoring information and associated documentation; Smart Grid information system audit records; documentation providing evidence of correlated information obtained from audit records and physical access monitoring records; security plan; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit review, analysis, and reporting responsibilities]. Test: [SELECT FROM: Smart Grid information system audit review, analysis, and reporting capability; Smart Grid information system capability integrating audit review, analysis, and reporting into an organizational process for investigation and response to suspicious activities; Smart Grid information system capability for centralizing review and analysis of audit records from multiple Smart Grid information system components].
SG.AU-7	Audit Reduction and Report Generation	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The Smart Grid information system provides an audit reduction and report generation capability. Supplemental Guidance Audit reduction and reporting may support near real-time analysis and after-the-fact investigations of security incidents. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system provides the capability to automatically process audit records for events of interest based on selectable event criteria	SG.AU-7.1 Determine if: (i) the Smart Grid information system provides audit reduction capabilities; and (ii) the Smart Grid information system provides report generation tools capabilities.	Examine, Interview, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit reduction and report generation; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; documented criteria for selectable events to audit; audit reduction, review, and reporting tools; Smart Grid information system audit records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit review, analysis, and reporting responsibilities]. Test: [SELECT FROM: Audit reduction and report generation capability].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AU-8	Time Stamps	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The Smart Grid information system uses internal system clocks to generate time stamps for audit records. Supplemental Guidance Time stamps generated by the information system include both date and time, as defined by the organization. Requirement Enhancements 1. The Smart Grid information system synchronizes internal Smart Grid information system clocks on an organization-defined frequency using an organization-defined time source. Additional Considerations	SG.AU-8.1 Determine if all Smart Grid information system components use internal system clocks to generate time stamps in audit records. SG.AU-8.2 (requirement enhancement 1) Determine if: (i) the organization defines a time source for clock synchronization; (ii) the organization defines the frequency for clock synchronization; and (iii) all Smart Grid information system components synchronize their clocks at the organization-defined frequency using an organization-defined time source.	Examine, Interview, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing time stamp generation; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit review, analysis, and reporting responsibilities]. Test: [SELECT FROM: Automated mechanisms implementing time stamp generation; Automated mechanisms implementing internal Smart Grid information system clock synchronization].
SG.AU-9	Protection of Audit Information	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The Smart Grid information system protects audit information and audit tools from unauthorized access, modification, and deletion. Supplemental Guidance Audit information includes, for example, audit records, audit settings, and audit reports. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system produces audit records on hardware-enforced, write-once media.	SG.AU-9.1 Determine if the Smart Grid information system protects audit information and audit tools from unauthorized access, modification, and deletion.	Examine, Interview, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation, Smart Grid information system audit records; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation, system or media storing backups of Smart Grid information system audit records; audit tools; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with auditing and accountability responsibilities]. Test: [SELECT FROM: Automated mechanisms implementing audit information protection; Media storage devices to hold audit records].
SG.AU-10	Audit Record Retention	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization retains audit logs for an organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations	SG.AU-10.1 Determine if: (i) the organization defines the retention period for audit records generated by the Smart Grid information system; and (ii) the organization retains Smart Grid information system audit records for the organization-defined time period to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit record retention; security plan; organization-defined retention period for audit records; Smart Grid information system audit records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit record retention responsibilities].
SG.AU-11	Conduct and Frequency of Audits	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization conducts audits on an organization-defined frequency to assess conformance to specified security requirements and applicable laws and regulations. Supplemental Guidance Audits can be either in the form of internal self-assessment (sometimes called first-party audits) or independent, third-party audits. Requirement Enhancements None. Additional Considerations	SG.AU-11.1 Determine if: (i) the organization defines the frequency of audits; (ii) the organization conducts audits in accordance with the organization-defined frequency; and (iii) the audits assess conformance to specified security requirements and applicable laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy and procedures; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with audit and accountability responsibilities].
SG.AU-12	Auditor Qualification	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization's audit program specifies auditor qualifications. Supplemental Guidance Security auditors need to— 1. Understand the Smart Grid information system and the associated operating practices; 2. Understand the risk involved with the audit; and 3. Understand the organization cyber security and the Smart Grid information system policy and procedures. Requirement Enhancements None. Additional Considerations A1. The organization assigns auditor and Smart Grid information system administration functions to separate personnel.	SG.AU-12.1 Determine if: (i) the organization's audit program specifies auditor qualifications; (ii) the organization selects auditors that understand the Smart Grid information system and associated operating practices; (iii) the organization selects auditors that understand the risks involved with the audit; (iv) the organization selects auditors that understand the organization cyber security and the Smart Grid information system policy and procedures; and (v) the organization selects auditors that are organizationally separated from the administration of the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy and procedures Auditor job description / qualification document; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with audit and accountability responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AU-13	Audit Tools	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization specifies the rules and conditions of use of audit tools. Supplemental Guidance Access to Smart Grid information systems audit tools needs to be protected to prevent any possible misuse or compromise. Requirement Enhancements None. Additional Considerations None.	SG.AU-13-1 Determine if the organization specifies the rules and conditions of use for audit tools	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit reduction and report generation; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; documented criteria for selectable events to audit; audit reduction, review, and reporting tools; Smart Grid information system audit records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit review, analysis, and reporting responsibilities].
SG.AU-14	Security Policy Compliance	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization demonstrates compliance to the organization's security policy through audits in accordance with the organization's audit program. Supplemental Guidance Periodic audits of the Smart Grid information system are implemented to demonstrate compliance to the organization's security policy. These audits— 1. Assess whether the defined cyber security policies and procedures, including those to identify security incidents, are being implemented and followed; 2. Document and ensure compliance to organization policies and procedures; 3. Identify security concerns, validate that the Smart Grid information system is free from security compromises, and provide information on the nature and extent of compromises should they occur; 4. Validate change management procedures and ensure that they produce an audit trail of reviews and approvals of all changes; 5. Verify that security mechanisms and management practices present during Smart Grid information system validation are still in place and functioning; 6. Ensure reliability and availability of the Smart Grid information system to support safe operation; and 7. Continuously improve performance. Requirement Enhancements None. Additional Considerations	SG.AU-14.1 Determine if the organization demonstrates compliance to the organization's security policy through audits in accordance with the organization's audit program.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.AU-15	Audit Generation	Tech	Category: Common Technical Requirements, Integrity Requirement The Smart Grid information system— 1. Provides audit record generation capability and generates audit records for the selected list of auditable events; and 2. Provides audit record generation capability and allows authorized users to select auditable events at the organization-defined Smart Grid information system components. Supplemental Guidance Audit records can be generated from various components within the Smart Grid information system. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system provides the capability to compile audit records from multiple components within the Smart Grid information system into a Smart Grid information system-wide audit trail that is time-correlated to within an organization-defined level of tolerance for relationship between time stamps of individual records in the audit trail.	SG.AU-15.1 Determine if: (i) the Smart Grid information system provides audit record generation capability for the selected list of auditable events; (ii) the Smart Grid information system generates audit records for the selected list of auditable events; (iii) the Smart Grid information system allows authorized users to select auditable events at the organization-defined Smart Grid information system components.	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit record generation; security plan; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit record generation responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.AU-16	Non-Repudiation	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system protects against an individual falsely denying having performed a particular action. Supplemental Guidance Non-repudiation protects individuals against later claims by an author of not having authored a particular document, a sender of not having transmitted a message, a receiver of not having received a message, or a signatory of not having signed a document. Non-repudiation services are implemented using various techniques (e.g., digital signatures, digital message receipts, and logging). Requirement Enhancements None. Additional Considerations None.	SG.AU-16.1 Determine if the Smart Grid information system protects against an individual falsely denying having performed a particular action.	Examine, Interview, Test	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing non-repudiation; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit record generation responsibilities]. Test: [SELECT FROM: Automated mechanisms implementing non-repudiation capability; Cryptographic mechanisms implementing digital signature capability within the Smart Grid information system].
			Security Assessment and Authorization (SG.CA)			
SG.CA-1	Security Assessment and Authorization Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented security assessment and authorization policy that addresses— i. The objectives, roles, and responsibilities for the security assessment and authorization security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the security assessment and authorization security program as it applies to all of the organizational staff and third-party contractors; and b. Procedures to address the implementation of the security assessment and authorization policy and associated security assessment and authorization protection requirements; 2. Management commitment ensures compliance with the organization's security assessment and authorization security policy and other regulatory requirements; and 3. The organization ensures that the security assessment and authorization security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The authorization to operate and security assessment policies can be included as part of the general information security policy for the organization. Authorization to operate and security assessment procedures can be developed for the security program in general and for a particular Smart Grid information system when required. The organization defines significant change to a Smart Grid information system for security reauthorizations. Requirement Enhancements None. Additional Considerations None.	SG.CA-1.1 Determine if the organization develops, implements, reviews, and updates on an organizational defined frequency a) A documented security assessment and authorization policy that addresses— i. the objectives, roles, and responsibilities for the security assessment and authorization security program as it relates to protecting the organization's personnel and assets; and ii. the scope of the security assessment and authorization security program as it applies to all of the organizational staff and third-party contractors; and b) Procedures to address the implementation of the security assessment and authorization policy and associated security assessment and authorization protection requirements. SG.CA-1.2 Determine if management commitment ensures compliance with the organization's security assessment and authorization security policy and other regulatory requirements. SG.CA-1.3 Determine if the organization ensures that the security assessment and authorization security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.CA-2	Security Assessments	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Develops a security assessment plan that describes the scope of the assessment including— a. Security requirements and requirement enhancements under assessment; b. Assessment procedures to be used to determine security requirement effectiveness; and c. Assessment environment, assessment team, and assessment roles and responsibilities; 2. Assesses the security requirements in the Smart Grid information system on an organization-defined frequency to determine the extent the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the Smart Grid information system; 3. Produces a security assessment report that documents the results of the assessment; and 4. Provides the results of the security requirements assessment to a management authority. Supplemental Guidance The organization assesses the security requirements in a Smart Grid information system as part of authorization or reauthorization to operate and continuous monitoring. Previous security assessment results may be reused to the extent that they are still valid and are supplemented with additional assessments as needed. Requirement Enhancements None.	SG.CA-2.1 Determine if the organization develops a security assessment plan that describes the scope of the assessment including— a) security requirements and requirement enhancements under assessment; b) assessment procedures to be used to determine security requirement effectiveness; and c) assessment environment, assessment team, and assessment roles and responsibilities. SG.CA-2.2 Determine if the organizations assesses the security requirements in the Smart Grid information system on an organization-defined frequency to determine the extent the requirements are a) implemented correctly; b) operating as intended; c) producing the desired outcome with respect to meeting the security requirements for the Smart Grid information system. SG.CA-2.3 Determine if the organization produces a security assessment report that documents the results of the assessment. SG.CA-2.4 Determine if the organization provides the results of the security requirements assessment to a management authority.	Examine, Interview	Examine: [SELECT FROM: Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security assessment responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.CA-3	Continuous Improvement	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization's security program implements continuous improvement practices to ensure that industry lessons learned and best practices are incorporated into Smart Grid information system security policies and procedures. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations -	SG.CA-3.1 Determine if the organization's security program implements continuous improvement practices to ensure that industry lessons learned and best practices are incorporated into Smart Grid information system security policies and procedures.	Examine, Interview	Examine: [SELECT FROM: Security assessment and authorization policy; procedures addressing security assessments; security plan; security assessment plan; security assessment report; security assessment evidence; plan of action and milestones; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security assessment responsibilities; organizational personnel with security management responsibilities].
SG.CA-4	Information System Connections	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Authorizes all connections from the Smart Grid information system to other information systems; 2. Documents the Smart Grid information system connections and associated security requirements for each connection; and 3. Monitors the Smart Grid information system connections on an ongoing basis, verifying enforcement of documented security requirements. Supplemental Guidance The organization considers the risk that may be introduced when a Smart Grid information system is connected to other information systems, both internal and external to the organization, with different security requirements. Risk considerations also include Smart Grid information systems sharing the same networks. Requirement Enhancements None. Additional Considerations A1. All external Smart Grid information system and communication connections are identified and protected from tampering or damage.	SG.CA-4.1 Determine if the organization authorizes all connections from the Smart Grid information system to other Smart Grid information systems. SG.CA-4.2 Determine if the organization documents the Smart Grid information system connections and associated security requirements for each connection. SG.CA-4.3 Determine if the organization monitors the Smart Grid information system connections on an ongoing basis, verifying enforcement of documented security requirements.	Examine, Interview	Examine: [SELECT FROM: Access control policy; procedures addressing Smart Grid information system connections; system and communications protection policy; Smart Grid information system interconnection security agreements; security plan; Smart Grid information system design documentation; security assessment report; plan of action and milestones; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibility for developing, implementing, or approving Smart Grid information system interconnection agreements].
SG.CA-5	Security Authorization to Operate	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization authorizes the Smart Grid information system for processing before operation and updates the authorization based on an organization-defined frequency or when a significant change occurs to the Smart Grid information system; and 2. A management authority signs and approves the security authorization to operate. Security assessments conducted in support of security authorizations need to be reviewed on an organization-defined frequency. Supplemental Guidance The organization assesses the security mechanisms implemented within the Smart Grid information system prior to security authorization to operate. Requirement Enhancements None. Additional Considerations	SG.CA-5.1 Determine if the organization authorizes the Smart Grid information system for processing before operation and updates the authorization based on an organization-defined frequency or when a significant change occurs to the Smart Grid information system. SG.CA-5.2 Determine if: (i) the organization documents a management authority to sign and approve the security authorization to operate; (ii) the documented management authority signs and approves the security authorization to operate (iii) the organization needs to conduct security assessments in support of security authorizations on an organization-defined frequency; (iv) the organization needs to review security assessments in support of security authorizations on an organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Security assessment and authorization policy; risk management policy; procedures addressing security authorization; security authorization package (including security plan; security assessment report; plan of action and milestones; authorization statement); other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security authorization responsibilities for Smart Grid information systems; organizational personnel with risk management responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.CA-6	Continuous Monitoring	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: 1. Ongoing security requirements assessments in accordance with the organizational continuous monitoring strategy; and 2. Reporting the security state of the Smart Grid information system to management authority on an organization-defined frequency. Supplemental Guidance A continuous monitoring program allows an organization to maintain the security authorization to operate of a Smart Grid information system over time in a dynamic operational environment with changing threats, vulnerabilities, technologies, and missions/business processes. The selection of an appropriate subset of security requirements for continuous monitoring is based on the impact level of the Smart Grid information system, the specific security requirements selected by the organization, and the level of assurance that the organization requires. Requirement Enhancements None. Additional Considerations A1. The organization employs an independent assessor or assessment team to monitor the security requirements in the Smart Grid information system on an ongoing basis; A2. The organization includes as part of security requirements continuous monitoring, periodic, unannounced, in-depth monitoring, penetration testing, and red team exercises; and A3. The organization uses automated support tools for continuous monitoring.	SG.CA-6.1 Determine if: (i) the organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes: a) ongoing security requirements assessments in accordance with the organizational continuous monitoring strategy; and b) reporting the security state of the Smart Grid information system to management authority on an organization-defined frequency; (ii) the organization documents the management authority receiving the security state reports of the Smart Grid information system; (iii) the organization defines the organizational frequency for reporting the security state of the Smart Grid information system to the management authority.	Examine, Interview, Test	Examine: [SELECT FROM: Security assessment and authorization policy; procedures addressing continuous monitoring of Smart Grid information system security controls; procedures addressing configuration management; security plan; security assessment report; plan of action and milestones; Smart Grid information system monitoring records; configuration management records, security impact analyses; status reports; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with continuous monitoring responsibilities; organizational personnel with configuration management responsibilities]. Test: [SELECT FROM: Automated mechanisms implementing monitoring capability within the Smart Grid information system].
			Configuration Management (SG.CM)			
SG.CM-1	Configuration Management Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented configuration management security policy that addresses— i. The objectives, roles, and responsibilities for the configuration management security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the configuration management security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the configuration management security policy and associated configuration management protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the configuration management security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The configuration management policy can be included as part of the general system security policy for the organization. Configuration management procedures can be developed for the security program in general and for a particular Smart Grid information system when required. Requirement Enhancements None.	SG.CM-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency— a) A documented configuration management security policy that addresses— 1) the objectives, roles, and responsibilities for the configuration management security program as it relates to protecting the organization's personnel and assets; and 2) the scope of the configuration management security program as it applies to all of the organizational staff, contractors, and third parties; and b) Procedures to address the implementation of the configuration management security policy and associated configuration management protection requirements. SG.CM-1.2 Determine if management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG.CM-1.3 Determine if the organization ensures that the configuration management security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.CM-2	Baseline Configuration	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization develops, documents, and maintains a current baseline configuration of the Smart Grid information system and an inventory of the Smart Grid information system's constituent components. The organization reviews and updates the baseline configuration as an integral part of Smart Grid information system component installations. Supplemental Guidance Maintaining the baseline configuration involves updating the baseline as the Smart Grid information system changes over time and keeping previous baselines for possible rollback. Requirement Enhancements None. Additional Considerations A1. The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration; and A2. The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the Smart Grid information system.	SG.CM-2.1 Determine if: (i) the organization a) develops the current baseline configuration of the Smart Grid information system; b) documents the current baseline configuration of the Smart Grid information system; c) maintains the current baseline configuration of the Smart Grid information system; d) implements the current baseline configuration of the Smart Grid information system; (ii) the organization maintains an inventory of the Smart Grid information system's constituent components; (iii) the organization reviews the baseline configuration as an integral part of Smart Grid information system component installations on an organizational defined frequency; (iv) the organization updates the baseline configuration as an integral part of Smart Grid information system component installations on an organizational defined frequency.	Examine, Interview	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the Smart Grid information system; list of software authorized to execute on the Smart Grid information system; enterprise / Smart Grid information system architecture documentation; Smart Grid information system design documentation; Smart Grid information system architecture and configuration documentation; historical copies of baseline configurations; security plan; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with configuration change control responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.CM-3	Configuration Change Control	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Authorizes and documents changes to the Smart Grid information system; 2. Retains and reviews records of configuration-managed changes to the Smart Grid information system; 3. Audits activities associated with configuration-managed changes to the Smart Grid information system; and 4. Tests, validates, and documents configuration changes (e.g., patches and updates) before installing them on the operational Smart Grid information system. Supplemental Guidance Configuration change control includes changes to the configuration settings for the Smart Grid information system and those IT products (e.g., operating systems, firewalls, routers) that are components of the Smart Grid information system. The organization includes emergency changes in the configuration change control process, including changes resulting from the remediation of flaws. Requirement Enhancements None. Additional Considerations None.	SG.CM-3.1 Determine if: (i) the organization documents changes to the Smart Grid information system; (ii) the organization authorizes changes to the Smart Grid information system. SG.CM-3.2 Determine if: (i) the organization retains records of configuration-managed changes to the Smart Grid information system; (ii) the organization reviews records of configuration-managed changes to the Smart Grid information system on an organizational defined frequency. SG.CM-3.3 Determine if the organization audits activities associated with configuration-managed changes to the Smart Grid information system. SG.CM-3.4 Determine if: (i) the organization tests configuration changes (e.g., patches and updates) before installing them on the operational Smart Grid information system; (ii) the organization validates configuration changes (e.g., patches and updates) before installing them on the operational Smart Grid information system; (iii) the organization documents configuration changes (e.g., patches and updates) before installing them on the operational Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing Smart Grid information system configuration change control; Smart Grid information system design documentation; Smart Grid information system architecture and configuration documentation; automated configuration control mechanisms; change control records; Smart Grid information system audit records; security plan; System and services acquisition policy; procedures addressing Smart Grid information system developer / integrator configuration management; acquisition contracts and service level agreements; Smart Grid information system developer / integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with configuration change control responsibilities; Organization personnel with Smart Grid information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities].
SG.CM-4	Monitoring Configuration Changes	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization implements a process to monitor changes to the Smart Grid information system; 2. Prior to change implementation and as part of the change approval process, the organization analyzes changes to the Smart Grid information system for potential security impacts; and 3. After the Smart Grid information system is changed, the organization checks the security features to ensure that the features are still functioning properly. Supplemental Guidance Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional safeguards and countermeasures are required. The organization considers Smart Grid information system safety and security interdependencies. Requirement Enhancements None. Additional Considerations	SG.CM-4.1 Determine if: (i) the organization documents a process to monitor changes to the Smart Grid information system; (ii) the organization implements a process to monitor changes to the Smart Grid information system. SG.CM-4.2 Determine if the organization, prior to change implementation and as part of the change approval process, analyzes changes to the Smart Grid information system for potential security impacts. SG.CM-4.3 Determine if the organization, after the Smart Grid information system is changed, checks the security features to ensure that the features are still functioning properly.	Examine, Interview, Test	Examine: [SELECT FROM: configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the Smart Grid information system; security impact analysis documentation; Smart Grid information system architecture and configuration documentation; change control records; Smart Grid information system audit records; security plan; System and services acquisition policy; procedures addressing Smart Grid information system developer / integrator configuration management; acquisition contracts and service level agreements; Smart Grid information system developer / integrator configuration management plan; security flaw tracking records; system change authorization records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for determining security impacts prior to implementation of Smart Grid information system changes; Organization personnel with Smart Grid information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities]. Test: [SELECT FROM: Automated mechanisms implementing configuration change
SG.CM-5	Access Restrictions for Configuration Change	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Defines, documents, and approves individual access privileges and enforces access restrictions associated with configuration changes to the Smart Grid information system; 2. Generates, retains, and reviews records reflecting all such changes; 3. Establishes terms and conditions for installing any hardware, firmware, or software on Smart Grid information system devices; and 4. Conducts audits of Smart Grid information system changes at an organization-defined frequency and if/when suspected unauthorized changes have occurred. Supplemental Guidance Planned or unplanned changes to the hardware, software, and/or firmware components of the Smart Grid information system may affect the overall security of the Smart Grid information system. Only authorized individuals should be allowed to obtain access to Smart Grid information system components for purposes of initiating changes, including upgrades, and modifications. Maintaining records is important for supporting after-the-fact actions should the organization become aware of an unauthorized change to the Smart Grid information system. Requirement Enhancements None. Additional Considerations A1. The organization employs automated mechanisms to enforce access restrictions and support auditing of the enforcement actions.	SG.CM-5.1 Determine if: (i) the organization defines individual access privileges associated with configuration changes to the Smart Grid information system; (ii) the organization documents individual access privileges associated with configuration changes to the Smart Grid information system; (iii) the organization approves individual access privileges associated with configuration changes to the Smart Grid information system; (iv) the organization enforces access restrictions associated with configuration changes to the Smart Grid information system. SG.CM-5.2 Determine if: (i) the organization generates records reflecting changes to individual access privileges on the Smart Grid information system; (ii) the organization retains records reflecting changes to individual access privileges on the Smart Grid information system; (iii) the organization reviews records reflecting changes to individual access privileges on the Smart Grid information system. SG.CM-5.3 Determine if the organization establishes terms and conditions for installing any hardware, firmware, or software on Smart Grid information system devices. SG.CM-5.4 Determine if the organization conducts audits of Smart Grid information system changes at an organization-defined frequency and if/when suspected unauthorized changes have occurred.	Examine, Interview, Test	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing access restrictions for changes to the Smart Grid information system; list of critical software programs to be prohibited from installation without an approved certificate; Smart Grid information system design documentation; security plan; Smart Grid information system architecture and configuration documentation; change control records; Smart Grid information system audit records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with logical access control responsibilities; organizational personnel with physical access control responsibilities; Organizational personnel responsible for enforcing a two-person rule for system changes]. Test: [SELECT FROM: Change control process and associated restrictions for changes to the Smart Grid information system; Automated mechanisms implementing access restrictions for changes to the Smart Grid information system; Smart Grid information system mechanisms preventing installation of software programs not signed with an organization-approved certificate; Smart Grid information system implementing safeguards and countermeasures for inappropriate changes to security functions].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.CM-6	Configuration Settings	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Establishes configuration settings for components within the Smart Grid information system; 2. Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures; 3. Documents changed configuration settings; 4. Identifies, documents, and approves exceptions from the configuration settings; and 5. Enforces the configuration settings in all components of the Smart Grid information system. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization employs automated mechanisms to centrally manage, apply, and verify configuration settings; A2. The organization employs automated mechanisms to respond to unauthorized changes to configuration settings; and A3. The organization incorporates detection of unauthorized, security-relevant configuration changes into the organization's incident response capability to ensure that such detected events are tracked, monitored, corrected, and available for historical purposes.	SG.CM-6.1 Determine if the organization establishes configuration settings for components within the Smart Grid information system. SG.CM-6.2 Determine if: (i) the organization monitors changes to the configuration settings in accordance with organizational policies and procedures; (ii) the organization controls changes to the configuration settings in accordance with organizational policies and procedures. SG.CM-6.3 Determine if the organization documents changed configuration settings. SG.CM-6.4 Determine if: (i) the organization identifies exceptions from the configuration settings; (ii) the organization documents exceptions from the configuration settings; (iii) the organization approves exceptions from the configuration settings. SG.CM-6.5 Determine if the organization enforces the configuration settings in all components of the Smart Grid information system.	Examine, Interview, Test	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing configuration settings for the Smart Grid information system; security plan; incident response plan; Smart Grid information system design documentation Smart Grid information system configuration settings and associated documentation; security configuration checklists; Smart Grid information system design documentation; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security configuration responsibilities; organization personnel with incident response planning responsibilities]. Test: [SELECT FROM: Automated mechanisms implementing the centralized management, application, and verification of configuration settings; Automated mechanisms implementing responses to unauthorized changes to configuration settings].
SG.CM-7	Configuration for Least Functionality	Tech	Category: Common Technical Requirements, Integrity Requirement 1. The organization configures the Smart Grid information system to provide only essential capabilities and specifically prohibits and/or restricts the use of functions, ports, protocols, and/or services as defined in an organizationally generated "prohibited and/or restricted" list; and 2. The organization reviews the Smart Grid information system on an organization-defined frequency or as deemed necessary to identify and restrict unnecessary functions, ports, protocols, and/or services. Supplemental Guidance The organization considers disabling unused or unnecessary physical and logical ports on Smart Grid information system components to prevent unauthorized connection of devices, and considers designing the overall system to enforce a policy of least functionality. Requirement Enhancements None. Additional Considerations	SG.CM-7.1 Determine if the organization configures the Smart Grid information system to provide only essential capabilities and specifically prohibits and / or restricts the use of functions, ports, protocols, and / or services as defined in an organizationally generated "prohibited and / or restricted" list. SG.CM-7.2 Determine if the organization reviews the Smart Grid information system on an organization-defined frequency or as deemed necessary to identify and restrict unnecessary functions, ports, protocols, and / or services.	Examine, Interview, Test	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing least functionality in the Smart Grid information system; security plan; Smart Grid information system design documentation; specification of preventing software program execution; Smart Grid information system configuration settings and associated documentation; security configuration checklists; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for identifying and eliminating unnecessary functions, ports, protocols, and services on the Smart Grid information system]. Test: [SELECT FROM: Smart Grid information system for disabling or restricting functions, ports, protocols, and services; Automated mechanisms preventing software program execution on the Smart Grid information system].
SG.CM-8	Component Inventory	Tech	Category: Common Technical Requirements, Integrity Requirement The organization develops, documents, and maintains an inventory of the components of the Smart Grid information system that— 1. Accurately reflects the current Smart Grid information system configuration; 2. Provides the proper level of granularity deemed necessary for tracking and reporting and for effective property accountability; 3. Identifies the roles responsible for component inventory; 4. Updates the inventory of system components as an integral part of component installations, system updates, and removals; and 5. Ensures that the location (logical and physical) of each component is included within the Smart Grid information system boundary. Supplemental Guidance The organization determines the appropriate level of granularity for any Smart Grid information system component included in the inventory that is subject to management control (e.g., tracking, reporting). Requirement Enhancements None. Additional Considerations A1. The organization updates the inventory of the information system components as an integral part of component installations and information system updates; A2. The organization employs automated mechanisms to maintain an up-to-date, complete, accurate, and readily available inventory of information system components; and A3. The organization employs automated mechanisms to detect the addition of unauthorized components or devise into the environment and disables access by components or devices or notifies designated officials	SG.CM-8.1 Determine if the organization develops, documents, and maintains an inventory of the components of the Smart Grid information system that— a) accurately reflects the current Smart Grid information system configuration; b) provides the proper level of granularity deemed necessary for tracking and reporting and for effective property accountability; c) identifies the roles responsible for component inventory; d) updates the inventory of system components as an integral part of component installations, system updates, and removals; e) ensures that the location (logical and physical) of each component is included within the Smart Grid information system boundary.	Examine, Interview, Test	Examine: [SELECT FROM: Configuration management policy; configuration management plan; ; Smart Grid information system design documentation; Smart Grid information system inventory records procedures addressing Smart Grid information system component inventory; security plan; Smart Grid information system inventory records; Smart Grid information system inventory records; component installation records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system inventory responsibilities; organizational personnel with responsibilities for defining Smart Grid information system components within the authorization boundary of the system; Organizational personnel with Smart Grid information system installation and inventory responsibilities]. Test: [SELECT FROM: Automated mechanisms implementing Smart Grid information system component inventory management; Automated mechanisms for detecting unauthorized components/devices on the Smart Grid information system].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.CM-9	Addition, Removal, and Disposal of Equipment	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization implements policy and procedures to address the addition, removal, and disposal of all Smart Grid information system equipment; and 2. All Smart Grid information system components and information are documented, identified, and tracked so that their location and function are known. Supplemental Guidance The policies and procedures should consider the sensitivity of critical security parameters such as passwords, cryptographic keys, and personally identifiable information such as name and social security numbers. Requirement Enhancements None. Additional Considerations	SG.CM-9.1 Determine if the organization implements policy and procedures to address the addition, removal, and disposal of all Smart Grid information system equipment. SG.CM-9.1 Determine if all Smart Grid information system components and information are documented, identified, and tracked so that their location and function are known.	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system media protection policy; media sanitization equipment test records; procedures addressing media sanitization and disposal; media sanitization records; audit records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media sanitization responsibilities].
SG.CM-10	Factory Default Settings Management	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization policy and procedures require the management of all factory default settings (e.g., authentication credentials, user names, configuration settings, and configuration parameters) on Smart Grid information system components and applications; and 2. The factory default settings should be changed upon installation and if used during maintenance. Supplemental Guidance Many Smart Grid information system devices and software are shipped with factory default settings to allow for initial installation and configuration. Requirement Enhancements None. Additional Considerations A1. The organization replaces default usernames whenever possible; and A2. Default passwords of applications, operating systems, database management systems, or other programs must be changed within an organizational-defined time period.	SG.CM-10.1 Determine if the organization policy and procedures require the management of all factory default settings (e.g., authentication credentials, user names, configuration settings, and configuration parameters) on Smart Grid information system components and applications. SG.CM-10.2 Determine if: (i) the factory default settings are changed upon installation; (ii) the factory default settings are change used during maintenance.	Examine, Interview, Test	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing responsibilities for configuration management process development; configuration standard documents; procedures addressing configuration management planning; security plan; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for configuration management process development]. Test: [SELECT FROM: Automated mechanisms implementing standardize configurations].
SG.CM-11	Configuration Management Plan	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization develops and implements a configuration management plan for the Smart Grid information system that— 1. Addresses roles, responsibilities, and configuration management processes and procedures; 2. Defines the configuration items for the Smart Grid information system; 3. Defines when (in the system development life cycle) the configuration items are placed under configuration management; 4. Defines the means for uniquely identifying configuration items throughout the system development life cycle; and 5. Defines the process for managing the configuration of the controlled items. Supplemental Guidance The configuration management plan defines processes and procedures for how configuration management is used to support system development life cycle activities. Requirement Enhancements None. Additional Considerations None.	SG.CM-11.1 Determine if the organization develops and implements a configuration management plan for the Smart Grid information system that— a) addresses roles, responsibilities, and configuration management processes and procedures; b) defines the configuration items for the Smart Grid information system; c) defines when (in the system development life cycle) the configuration items are placed under configuration management; d) defines the means for uniquely identifying configuration items throughout the system development life cycle; e) defines the process for managing the configuration of the controlled items.	Examine, Interview	Examine: [SELECT FROM: Configuration management policy; configuration management plan; procedures addressing responsibilities for configuration management process development; procedures addressing configuration management planning; security plan; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for configuration management process development].
Continuity of Operations (SG.CP)						

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.CP-1	Continuity of Operations Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented continuity of operations security policy that addresses— i. The objectives, roles, and responsibilities for the continuity of operations security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the continuity of operations security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the continuity of operations security policy and associated continuity of operations protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the continuity of operations security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The continuity of operations policy can be included as part of the general information security policy for the organization. Continuity of operations procedures can be developed for the security program in general, and for a particular Smart Grid information system, when required. Requirement Enhancements None.	SG.CP-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency— a) a documented continuity of operations security policy that addresses— 1) the objectives, roles, and responsibilities for the continuity of operations security program as it relates to protecting the organization's personnel and assets; and 2) the scope of the continuity of operations security program as it applies to all of the organizational staff, contractors, and third parties; and b) procedures to address the implementation of the continuity of operations security policy and associated continuity of operations protection requirements. SG.CP-1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirements; and (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG.CP-1.3 Determine if the organization ensures that the continuity of operations security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.CP-2	Continuity of Operations Plan	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops and implements a continuity of operations plan dealing with the overall issue of maintaining or reestablishing operations in case of an undesirable interruption for a Smart Grid information system; 2. The plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring Smart Grid information system operations after a disruption or failure; and 3. A management authority reviews and approves the continuity of operations plan. Supplemental Guidance A continuity of operations plan addresses both business continuity planning and recovery of Smart Grid information system operations. Development of a continuity of operations plan is a process to identify procedures for safe Smart Grid information system operation while recovering from a Smart Grid information system disruption. The plan requires documentation of critical Smart Grid information system functions that need to be recovered. Requirement Enhancements None. Additional Considerations A1. The organization performs a root cause analysis for the event and submits any findings from the analysis to management.	SG.CP-2.1 Determine if: (i) the organization develops a continuity of operations plan dealing with the overall issue of maintaining or reestablishing operations in case of an undesirable interruption for a Smart Grid information system; (ii) the organization documents a continuity of operations plan dealing with the overall issue of maintaining or reestablishing operations in case of an undesirable interruption for a Smart Grid information system; (iii) the organization implements a continuity of operations plan dealing with the overall issue of maintaining or reestablishing operations in case of an undesirable interruption for a Smart Grid information system. SG.CP-2.2 Determine if the organizational continuity of operations plan addresses roles, responsibilities, assigned individuals with contact information, and activities associated with restoring Smart Grid information system operations after a disruption or failure. SG.CP-2.3 Determine if: (i) the organization document a management authority for the continuity of operations plan; (ii) the management authority reviews and approves the continuity of operations plan.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy and procedures; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with contingency planning responsibilities].
SG.CP-3	Continuity of Operations Roles and Responsibilities	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The continuity of operations plan— 1. Defines the roles and responsibilities of the various employees and contractors in the event of a significant incident; and 2. Identifies responsible personnel to lead the recovery and response effort if an incident occurs. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations None.	SG.CP-3.1 Determine if the organizational continuity of operations plan for Smart Grid information systems a) defines the roles and responsibilities of the various employees and contractors in the event of a significant incident; and b) identifies responsible personnel to lead the recovery and response effort if an incident occurs.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy; procedures addressing contingency operations for the Smart Grid information system; contingency plan; security plan; business impact assessment; other related plans; alternate processing site agreements; alternate storage site agreements; contingency plan testing and / or exercise documentation; contingency plan test results; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas; organizational personnel with incident handling responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.CP-4	Continuity of Operations Training	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization trains personnel in their continuity of operations roles and responsibilities with respect to the Smart Grid information system and provides refresher training on an organization-defined frequency. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations	SG.CP-4.1 Determine if: (i) the organization trains personnel in their continuity of operations roles and responsibilities with respect to the Smart Grid information system; (ii) the organization provides refresher training on their continuity of operations roles and responsibility with respect to the Smart Grid information system on an organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing contingency training; contingency training curriculum; contingency training material; security plan; contingency training records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with contingency planning, plan implementation, and training responsibilities].
SG.CP-5	Continuity of Operations Plan Testing	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The continuity of operations plan is tested to determine its effectiveness and results are documented; 2. A management authority reviews the documented test results and initiates corrective actions, if necessary; and 3. The organization tests the continuity of operations plan for the Smart Grid information system on an organization-defined frequency, using defined tests. Supplemental Guidance None. Requirement Enhancements 1. The organization coordinates continuity of operations plan testing and exercises with all affected organizational elements. Additional Considerations A1. The organization employs automated mechanisms to test/exercise the continuity of operations plan; and A2. The organization tests/exercises the continuity of operations plan at the alternate processing site to familiarize Smart Grid information system operations personnel with the facility and available resources and to evaluate the site's capabilities to support continuity of operations.	SG.CP-5.1 Determine if: (i) the continuity of operations plan is tested to determine its effectiveness; (ii) the continuity of operations plan testing results are documents. SG.CP-5.2 Determine if: (i) the organization documented a management authority to review continuity of operations plan test results (ii) the management authority reviews the documented test results and initiates corrective actions, if necessary. SG.CP-5.3 Determine if the organization tests the continuity of operations plan for the Smart Grid information system on an organization-defined frequency, using defined tests. SG.CP-5.4 (requirement enhancements 1) Determine if the organization coordinates continuity of operations plan testing and exercises with all affected organizational elements.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy; contingency plan, procedures addressing contingency plan testing and exercises; security plan; automated mechanisms supporting contingency plan testing/exercises; contingency plan testing and / or exercise documentation; contingency plan test results; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for reviewing or responding to contingency plan tests/exercises; Organizational personnel with Smart Grid information system recovery and reconstitution responsibilities; organizational personnel with contingency plan testing and / or exercise responsibilities; Organizational personnel with contingency planning, plan implementation, and testing responsibilities; organizational personnel with responsibilities for related plans].
SG.CP-6	Continuity of Operations Plan Update	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization reviews the continuity of operations plan for the Smart Grid information system and updates the plan to address Smart Grid information system, organizational, and technology changes or problems encountered during plan implementation, execution, or testing on an organization-defined frequency. Supplemental Guidance Organizational changes include changes in mission, functions, or business processes supported by the Smart Grid information system. The organization communicates the changes to appropriate organizational elements. Requirement Enhancements None. Additional Considerations	SG.CP-6.1 Determine if: (i) the organization reviews the continuity of operations plan for the Smart Grid information system on an organizational defined frequency; (ii) the organization updates the continuity of operations plan to address Smart Grid information system, organizational, and technology changes or problems encountered during plan implementation, execution, or testing on an organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy; procedures addressing contingency operations for the Smart Grid information system; contingency plan; security plan; business impact assessment; other related plans; alternate processing site agreements; alternate storage site agreements; contingency plan testing and / or exercise documentation; contingency plan test results; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas; organizational personnel with incident handling responsibilities].
SG.CP-7	Alternate Storage Sites	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization determines the requirement for an alternate storage site and initiates any necessary agreements. Supplemental Guidance The Smart Grid information system backups and the transfer rate of backup information to the alternate storage site are performed on an organization-defined frequency. Requirement Enhancements 1. The organization identifies potential accessibility problems at the alternative storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions; 2. The organization identifies an alternate storage site that is geographically separated from the primary storage site so it is not susceptible to the same hazards; and 3. The organization configures the alternate storage site to facilitate timely and effective recovery operations. Additional Considerations	SG.CP-7.1 Determine if: (i) the organization determines the requirement for an alternate storage site for continuity of operations; (ii) the organization initiates any necessary agreements for an alternate storage site for continuity of operations. SG.CP-7.2 (requirement enhancements 1) Determine if the organization identifies potential accessibility problems at the alternative storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. SG.CP-7.3 (requirement enhancements 2) Determine if the organization identifies an alternate storage site that is geographically separated from the primary storage site so it is not susceptible to the same hazards. SG.CP-7.4 (requirement enhancements 3) Determine if the organization configures the alternate storage site to facilitate timely and effective recovery operations.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing alternate storage sites; alternate storage site; alternate storage site agreements; mitigation actions for accessibility problems to the alternate storage site; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities and responsibilities in related plan areas; organizational personnel with incident handling responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.CP-8	Alternate Telecommunication Services	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization identifies alternate telecommunication services for the Smart Grid information system and initiates necessary agreements to permit the resumption of operations for the safe operation of the Smart Grid information system within an organization-defined time period when the primary Smart Grid information system capabilities are unavailable. Supplemental Guidance Alternate telecommunication services required to resume operations within the organization-defined time period are either available at alternate organization sites or contracts with vendors need to be in place to support alternate telecommunication services for the Smart Grid information system. Requirement Enhancements 1. Primary and alternate telecommunication service agreements contain priority-of-service provisions in accordance with the organization's availability requirements; 2. Alternate telecommunication services do not share a single point of failure with primary telecommunication services; 3. Alternate telecommunication service providers need to be sufficiently separated from primary service providers so they are not susceptible to the same hazards; and 4. Primary and alternate telecommunication service providers need to have adequate contingency plans. Additional Considerations None.	SG.CP-8.1 Determine if: (i) the organization identifies alternate telecommunication services for the Smart Grid information system for continuity of operations; (ii) the organization initiates necessary agreements to permit the resumption of operations for the safe operation of the Smart Grid information system within an organization-defined time period when the primary Smart Grid information system capabilities are unavailable. SG.CP-8.2 (requirement enhancement 1) Determine if: (i) primary telecommunication service agreements contain priority-of-service provisions in accordance with the organization's availability requirements; (ii) alternate telecommunication service agreements contain priority-of-service provisions in accordance with the organization's availability requirements. SG.CP-8.3 (requirement enhancement 2) Determine if alternate telecommunication services do not share a single point of failure with primary telecommunication services. SG.CP-8.4 (requirement enhancement 3) Determine if alternate telecommunication service providers need to be sufficiently separated from primary service providers so they are not susceptible to the same hazards. SG.CP-8.5 (requirement enhancement 4) Determine if (i) primary telecommunication service providers need to have adequate contingency plans; (ii) alternate telecommunication service providers need to have adequate contingency plans.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; security plan; primary and alternate telecommunications service agreements; Telecommunications Service Priority documentation; list of essential missions and business functions; primary telecommunications service provider's site; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with contingency planning, plan implementation, and testing responsibilities; telecommunications service providers].
SG.CP-9	Alternate Control Center	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization identifies an alternate control center, necessary telecommunications, and initiates any necessary agreements to permit the resumption of Smart Grid information system operations for critical functions within an organization-prescribed time period when the primary control center is unavailable. Supplemental Guidance Equipment, telecommunications, and supplies required to resume operations within the organization-prescribed time period need to be available at the alternative control center or by a contract in place to support delivery to the site. Requirement Enhancements 1. The organization identifies an alternate control center that is geographically separated from the primary control center so it is not susceptible to the same hazards; 2. The organization identifies potential accessibility problems to the alternate control center in the event of an area-wide disruption or disaster and outlines explicit mitigation actions; and 3. The organization develops alternate control center agreements that contain priority-of-service provisions in accordance with the organization's availability requirements. Additional Considerations A1. The organization fully configures the alternate control center and telecommunications so that they are ready to be used as the operational site supporting a minimum required operational capability; and A2. The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.	SG.CP-9.1 Determine if the organization identifies an alternate control center to permit the resumption of Smart Grid information system operations for critical functions within an organization-prescribed time period when the primary control center is unavailable that includes a) necessary telecommunications b) initiates any necessary agreements. SG.CP-9.2 (requirement enhancements 1) Determine if the organization identifies an alternate control center that is geographically separated from the primary control center so it is not susceptible to the same hazards for continuity of operations. SG.CP-9.3 (requirement enhancements 2) Determine if the organization identifies potential accessibility problems to the alternate control center in the event of an area-wide disruption or disaster and outlines explicit mitigation actions. SG.CP-9.4 (requirement enhancements 3) Determine if the organization develops alternate control center agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing alternate telecommunications services; security plan; primary and alternate telecommunications service agreements; Telecommunications Service Priority documentation; list of essential missions and business functions; primary telecommunications service provider's site; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with contingency planning, plan implementation, and testing responsibilities; telecommunications service providers].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.CP-10	Smart Grid Information System Recovery and Reconstitution	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization provides the capability to recover and reconstitute the Smart Grid information system to a known secure state after a disruption, compromise, or failure. Supplemental Guidance Smart Grid information system recovery and reconstitution to a known secure state means that— 1. All Smart Grid information system parameters (either default or organization-established) are set to secure values; 2. Security-critical patches are reinstalled; 3. Security-related configuration settings are reestablished; 4. Smart Grid information system documentation and operating procedures are available; 5. Application and Smart Grid information system software is reinstalled and configured with secure settings; 6. Information from the most recent, known secure backups is loaded; and 7. The Smart Grid information system is fully tested. Requirement Enhancements 1. The organization provides compensating security controls (including procedures or mechanisms) for the organization-defined circumstances that inhibit recovery to a known, secure state; and 2. The organization provides the capability to reimage Smart Grid information system components in accordance with organization-defined restoration time periods from configuration-controlled and integrity-protected media images representing a secure, operational state for the components. Additional Considerations None.	SG.CP-10.1 Determine if: (i) the organization provides the capability to recover and reconstitute the Smart Grid information system to a known secure state after a disruption, compromise, or failure; (ii) the organization documents the Smart Grid information system secure state. SG.CP-10.2 (requirement enhancement 1) Determine if the organization provides compensating security controls (including procedures or mechanisms) for the organization-defined circumstances that inhibit recovery to a known, secure state. SG.CP-10.3 (requirement enhancement 2) Determine if the organization provides the capability to reimage Smart Grid information system components in accordance with organization-defined restoration time periods from configuration-controlled and integrity-protected media images representing a secure, operational state for the components.	Examine, Interview, Test	Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing Smart Grid information system recovery and reconstitution; Smart Grid information system configuration settings and associated documentation; Smart Grid information system design documentation; Smart Grid information system design documentation; contingency plan test results; location(s) of backup and restoration hardware, firmware, and software; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system recovery and reconstitution responsibilities]. Test: [SELECT FROM: Automated mechanisms and / or manual procedures for implementing Smart Grid information system recovery and reconstitution operations; Failover capability for the Smart Grid information system].
SG.CP-11	Fail-Safe Response	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The Smart Grid information system has the ability to execute an appropriate fail-safe procedure upon the loss of communications with other Smart Grid information systems or the loss of the Smart Grid information system itself. Supplemental Guidance In the event of a loss of communication between the Smart Grid information system and the operational facilities, the on-site instrumentation needs to be capable of executing a procedure that provides the maximum protection to the controlled infrastructure. For the electric sector, this may be to alert the operator of the failure and then do nothing (i.e., let the electric grid continue to operate). The organization defines what “loss of communications” means (e.g., 5 seconds or 5 minutes without communications). The organization then defines the appropriate fail-safe process for its industry. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system preserves the organization-defined state information in failure.	SG.CP-11.1 Determine if the Smart Grid information system has the ability to execute an appropriate fail-safe procedure upon the loss of communications with other Smart Grid information systems or the loss of the Smart Grid information system itself.	Examine, Interview, Test	Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing Smart Grid information system recovery and reconstitution; Smart Grid information system configuration settings and associated documentation; Smart Grid information system design documentation; Smart Grid information system design documentation; contingency plan test results; location(s) of backup and restoration hardware, firmware, and software; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system recovery and reconstitution responsibilities]. Test: [SELECT FROM: Automated mechanisms and / or manual procedures for implementing Smart Grid information system recovery and reconstitution operations; Failover capability for the Smart Grid information system].
Identification and Authentication (SG.IA)						
SG.IA-1	Identification and Authentication Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented identification and authentication security policy that addresses— i. The objectives, roles, and responsibilities for the identification and authentication security program as it relates to protecting the organization’s personnel and assets; and ii. The scope of the identification and authentication security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the identification and authentication security policy and associated identification and authentication protection requirements; 2. Management commitment ensures compliance with the organization’s security policy and other regulatory requirements; and 3. The organization ensures that the identification and authentication security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The identification and authentication policy can be included as part of the general security policy for the organization. Identification and authentication procedures can be developed for the security program in general and for a particular Smart Grid information system when required. Requirement Enhancements None. Additional Considerations None.	SG.IA-1.1 Determine if: (i) the organization develops and implements a documented identification and authentication policy; (ii) the identification and authentication policy addresses identification and authentication as it related to protecting the organization’s personnel and assets and the following: a) purpose / objective b) scope c) roles and responsibilities d) coordination among organizational entities, and compliance; (iii) the identification and authentication policy addresses the scope to include all organizational staff, contractors, and third parties; (iv) the organization develops and implements the identification and authentication procedures; (v) the organization reviews and updates the identification and authentication procedures (COVERED inSG.IA.2(i)); (vi) management commitment ensures compliance with the organization’s identification and authentication policy, security policy and other regulatory requirements; (vii) the identification and authentication policy comply with applicable federal, state, local, tribal, and territorial laws and regulations; and (viii) the identification and authentication procedures facilitate implementation of the identification and authentication security policy. SG.IA-1.2 Determine if: (i) the organization defines the frequency of identification and authentication policy and procedures reviews/updates; (ii) the organization reviews/updates the identification and authentication policy and procedures in accordance with the organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.IA-2	Identifier Management	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization receives authorization from a management authority to assign a user or device identifier. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization archives previous user or device identifiers; and A2. The organization selects an identifier that uniquely identifies an individual or device.	SG.IA-2.1 Determine if the organization received authorization from a management authority to assign a user or device identifier.	Examine, Interview, Test	Examine: [SELECT FROM: Identification and authentication policy; procedures addressing identifier management; procedures addressing account management; security plan; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; list of Smart Grid information system accounts; list of characteristics identifying user status; list of identifiers generated from physical access control devices; identifier certification documentation; organizational personnel biometrics records; procedures addressing account management; user ID and password registration documentation; ID and password authorization records; registration authority records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with identifier management responsibilities]. Test: [SELECT FROM: Automated mechanisms implementing identifier management functions].
SG.IA-3	Authenticator Management	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization manages Smart Grid information system authentication credentials for users and devices by— 1. Defining initial authentication credential content, such as defining password length and composition, tokens; 2. Establishing administrative procedures for initial authentication credential distribution; lost, compromised, or damaged authentication credentials; and revoking authentication credentials; 3. Changing/refreshing authentication credentials on an organization-defined frequency; and 4. Specifying measures to safeguard authentication credentials. Supplemental Guidance Measures to safeguard user authentication credentials include maintaining possession of individual authentication credentials, not loaning or sharing authentication credentials with others, and reporting lost or compromised authentication credentials immediately. Requirement Enhancements None. Additional Considerations A1. The organization employs automated tools to determine if authentication credentials are sufficiently strong to resist attacks intended to discover or otherwise compromise the authentication credentials; and A2. The organization requires unique authentication credentials be provided by vendors and manufacturers of Smart Grid information system components.	SG-IA-3.1 Determine if the organization manages the Smart Grid information system authentication credential for users and devices by (a) defining initial authentication credential content, such as defining password length and composition, tokens; (b) establishing administrative procedures for 1) initial authentication credential distribution 2) lost, compromised, or damaged authentication credentials 3) revoking authentication credentials; (c) Changing/refreshing authentication credentials on an organization-defined frequency; and (d) Specifying measures to safeguard authentication credentials. SG-IA-3.2 Determine if the organization defines the frequency for authentication credential changing / refreshing.	Examine, Interview, Test	Examine: [SELECT FROM: Identification and authentication policy; procedures addressing authenticator management; list of authenticators that require in-person registration; authenticator registration documentation; Smart Grid information system design documentation; system and services acquisition policy; procedures addressing authenticator management; procedures addressing the integration of security requirements into the acquisition process; acquisition documentation; acquisition contracts for Smart Grid information system procurements or services; Smart Grid information system configuration settings and associated documentation; logical access scripts; automated tools for testing authenticators; application code reviews for detecting unencrypted static authenticators; security plan; list of individuals having accounts on multiple Smart Grid information systems; information classification or sensitivity documentation; security categorization documentation for the Smart Grid information system; security assessments of authenticator protections; risk assessment results; list of measures intended to manage risk of compromise due to individuals having accounts on multiple Smart Grid information systems; PKI certification revocation lists; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for determining initial authenticator content; Organizational personnel with authenticator management responsibilities; organizational personnel implementing and / or maintaining authenticator protections; Organizational personnel with responsibilities for PKI-based authentication management; organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities].
SG.IA-4	User Identification and Authentication	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system uniquely identifies and authenticates users (or processes acting on behalf of users). Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system uses multifactor authentication for— a. Remote access to non-privileged accounts; b. Local access to privileged accounts; and c. Remote access to privileged accounts.	SG.IA-4.1 Determine if: (i) the organization uniquely identifies users; (ii) the organization authenticates users.	Examine, Interview, Test	Examine: [SELECT FROM: Identification and authentication policy; procedures addressing user identification and authentication; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; list of Smart Grid information system accounts; list of privileged Smart Grid information system accounts; list of non-privileged Smart Grid information system accounts; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for determining initial authenticator content; Organizational personnel with authenticator management responsibilities; organizational personnel implementing and / or maintaining authenticator protections; Organizational personnel with responsibilities for PKI-based authentication management; organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities]. Test: [SELECT FROM: Automated mechanisms implementing identification and authentication capability for the Smart Grid information system].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.IA-5	Device Identification and Authentication	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system uniquely identifies and authenticates an organization-defined list of devices before establishing a connection. Supplemental Guidance The devices requiring unique identification and authentication may be defined by type, by specific device, or by a combination of type and device as deemed appropriate by the organization. Requirement Enhancements 1. The Smart Grid information system authenticates devices before establishing remote network connections using bidirectional authentication between devices that is cryptographically based; and 2. The Smart Grid information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based. Additional Considerations	SG.IA-5.1 Determine if: (i) the organization uniquely identified an organization-defined list of devices before establishing a connection; (ii) the organization authenticates an organization-defined list of devices before establishing a connection. SG.IA-5.1 Determine if: (i) The Smart Grid information system authenticates devices before establishing remote network connections using bidirectional authentication between devices that is cryptographically based; (ii) the Smart Grid information system authenticates devices before establishing network connections using bidirectional authentication between devices that is cryptographically based.	Examine, Interview, Test	Examine: [SELECT FROM: Identification and authentication policy; procedures addressing device identification and authentication; Smart Grid information system design documentation; list of devices requiring unique identification and authentication; device connection reports; Smart Grid information system configuration settings and associated documentation; DHCP lease information; device connection reports; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for determining initial authenticator content; Organizational personnel with authenticator management responsibilities; organizational personnel implementing and / or maintaining authenticator protections; Organizational personnel with responsibilities for PKI-based authentication management; organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities]. Test: [SELECT FROM: Automated mechanisms implementing device identification and authentication].
SG.IA-6	Authenticator Feedback	Tech	Category: Unique Technical Requirements Requirement The authentication mechanisms in the Smart Grid information system obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals. Supplemental Guidance The Smart Grid information system obscures feedback of authentication information during the authentication process (e.g., displaying asterisks when a user types in a password). The feedback from the Smart Grid information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Requirement Enhancements None. Additional Considerations None.	SG.IA-6.1 Determine if the organization authentication mechanisms in the Smart Grid information system obscure feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	Examine, Test	Examine: [SELECT FROM: Identification and authentication policy; procedures addressing authenticator feedback; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing authenticator feedback].
Information and Document Management (SG.ID)						
SG.ID-1	Information and Document Management Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A Smart Grid information and document management policy that addresses— i. The objectives, roles and responsibilities for the information and document management security program as it relates to protecting the organization's personnel and assets; ii. The scope of the information and document management security program as it applies to all the organizational staff, contractors, and third parties; iii. The retrieval of written and electronic records, equipment, and other media for the Smart Grid information system; and iv. The destruction of written and electronic records, equipment, and other media for the Smart Grid information system; and b. Procedures to address the implementation of the information and document management security policy and associated Smart Grid information system information and document management protection requirements; 2. Management commitment ensures compliance of the organization's security policy and other regulatory requirements; and 3. The organization ensures that the Smart Grid information system information and document management policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The information and document management policy may be included as part of the general information security policy for the organization. The information and document management procedures can be developed for the security program in general and for a particular Smart Grid information system when required. The organization employs appropriate measures to ensure that long-term records and information can be retrieved (e.g., converting the data to a newer format, retaining older equipment that can read the data). Destruction includes the method of disposal such as shredding of paper records, erasing of disks or other electronic media, or physical destruction. Requirement Enhancements None. Additional Considerations None.	SG.ID-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency— a) a Smart Grid information and document management policy that addresses— 1) the objectives, roles and responsibilities for the information and document management security program as it relates to protecting the organization's personnel and assets; 2) the scope of the information and document management security program as it applies to all the organizational staff, contractors, and third parties; 3) the retrieval of written and electronic records, equipment, and other media for the Smart Grid information system; and 4) the destruction of written and electronic records, equipment, and other media for the Smart Grid information system; and b) procedures to address the implementation of the information and document management security policy and associated Smart Grid information system information and document management protection requirements. SG.ID-1.2 Determine if management commitment ensures compliance of the organization's security policy and other regulatory requirements. SG.ID-1.3 Determine if the organization ensures that the Smart Grid information system information and document management policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.ID-2	Information and Document Retention	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops policies and procedures detailing the retention of organization information; 2. The organization performs legal reviews of the retention policies to ensure compliance with all applicable laws and regulations; 3. The organization manages Smart Grid information system-related data including establishing retention policies and procedures for both electronic and paper data; and 4. The organization manages access to Smart Grid information system-related data based on assigned roles and responsibilities. Supplemental Guidance The retention procedures address retention/destruction issues for all applicable information media. Requirement Enhancements None. Additional Considerations None.	SG.ID-2.1 Determine if the organization develops policies and procedures detailing the retention of organization information. SG.ID-2.2 Determine if the organization performs legal reviews of the retention policies to ensure compliance with all applicable laws and regulations. SG.ID-2.3 Determine if the organization manages Smart Grid information system-related data including establishing retention policies and procedures for both electronic and paper data. SG.ID-2.4 Determine if the organization manages access to Smart Grid information system-related data based on assigned roles and responsibilities.	Examine, Interview	Examine: [SELECT FROM: Audit and accountability policy; procedures addressing audit record retention; security plan; organization-defined retention period for audit records; Smart Grid information system audit records System and information integrity policy; procedures addressing Smart Grid information system output handling and retention; media protection policy and procedures; information retention records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system audit record retention responsibilities; Organizational personnel with information output handling and retention responsibilities].
SG.ID-3	Information Handling	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement Organization-implemented policies and procedures detailing the handling of information are developed and reviewed on an organization-defined frequency. Supplemental Guidance Written policies and procedures detail access, sharing, copying, transmittal, distribution, and disposal or destruction of Smart Grid information system information. These policies or procedures include the periodic review of all information to ensure that it is properly handled. Requirement Enhancements None. Additional Considerations	SG.ID-3.1 Determine if: (i) the organization-implemented policies and procedures detailing the handling of information are developed; (ii) the organization-implemented policies and procedures detailing the handling of information are reviewed on an organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Media protection policy and procedures; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media protection responsibilities].
SG.ID-4	Information Exchange	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement Agreements are established for the exchange of information, firmware, and software between the organization and external parties such as third parties, vendors and contractors. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. If a specific device needs to communicate with another device outside the Smart Grid information system, communications need to be limited to only the devices that need to communicate.	SG.ID-4.1 Determine if organizational agreements are established for the exchange of information, firmware, and software between the organization and external parties such as third parties, vendors and contractors.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; access control policy; contingency planning policy; security plan for the Smart Grid information system; contingency plan for the Smart Grid information system; Smart Grid information system design documentation; boundary protection procedures; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; procedures addressing the use of external Smart Grid information systems; security plan; Smart Grid information system connection or processing agreements; other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with security planning and plan implementation responsibilities for the Smart Grid information system; Organizational personnel with responsibility for developing, implementing, or approving Smart Grid information system interconnection agreements].
SG.ID-5	Automated Labeling	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The Smart Grid information system automatically labels information in storage, in process, and in transmission in accordance with— 1. Access control requirements; 2. Special dissemination, handling, or distribution instructions; and 3. Otherwise as required by the Smart Grid information system security policy. Supplemental Guidance Automated labeling refers to labels employed on internal data structures (e.g., records, buffers, files) within the Smart Grid information system. Such labels are often used to implement access control and flow control policies. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system maintains the binding of the label to the information.	SG.ID-5.1 Determine if the Smart Grid information system automatically labels information in storage, in process, and in transmission in accordance with— a) access control requirements; b) special dissemination, handling, or distribution instructions; and c) otherwise as required by the Smart Grid information system security policy.	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system marking protection policy; procedures addressing information labeling; security plan; storage media and Smart Grid information system output; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system information protection and marking responsibilities].
Incident Response (SG.IR)						

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.IR-1	Incident Response Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented incident response security policy that addresses— i. The objectives, roles, and responsibilities for the incident response security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the incident response security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the incident response security policy and associated incident response protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; 3. The organization ensures that the incident response security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations; and 4. The organization identifies potential interruptions and classifies them as to "cause," "effects," and "likelihood." Supplemental Guidance The incident response policy can be included as part of the general information security policy for the organization. Incident response procedures can be developed for the security program in general, and for a particular Smart Grid information system, when required. The various types of incidents that may result from system intrusion need to be identified and classified as to their effects and likelihood so that a proper response can be formulated for each potential incident. The organization determines the impact to each Smart Grid system and the consequences associated with loss of one or more of the Smart Grid information systems. Requirement Enhancements None. Additional Considerations None.	SG.IR-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency— a) a documented incident response security policy that addresses— 1) the objectives, roles, and responsibilities for the incident response security program as it relates to protecting the organization's personnel and assets; and 2) the scope of the incident response security program as it applies to all of the organizational staff, contractors, and third parties; and b) procedures to address the implementation of the incident response security policy and associated incident response protection requirements. SG.IR-1.2 Determine if: (i) the organization documents management's commitment to ensure compliance with the organization's security policy and other regulatory requirements; (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG.IR-1.3 Determine if the organization ensures that the incident response security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. SG.IR-1.4 Determine if the organization identifies potential interruptions and classifies them as to "cause," "effects," and "likelihood."	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.IR-2	Incident Response Roles and Responsibilities	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization's Smart Grid information system security plan defines the specific roles and responsibilities in relation to various types of incidents; and 2. The plan identifies responsible personnel to lead the response effort if an incident occurs. Response teams need to be formed, including Smart Grid information system and other process owners, to reestablish operations. Supplemental Guidance The organization's Smart Grid information system security plan defines the roles and responsibilities of the various employees, contractors, and third parties in the event of an incident. The response teams have a major role in the interruption identification and planning process. Requirement Enhancements None. Additional Considerations None.	SG.IR-2.1 Determine if the organization's Smart Grid information system security plan defines the specific roles and responsibilities in relation to various types of incidents. SG.IR-2.2 Determine if: (i) the plan identifies responsible personnel to lead the response effort if an incident occurs; (ii) the organization forms documents response teams to include Smart Grid information system and other process owners, to reestablish operations.	Examine, Interview	Examine: [SELECT FROM: Incident response policy and procedures; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident response responsibilities].
SG.IR-3	Incident Response Training	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement Personnel are trained in their incident response roles and responsibilities with respect to the Smart Grid information system and receive refresher training on an organization-defined frequency. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization incorporates Smart Grid information system simulated events into continuity of operations training to facilitate effective response by personnel in crisis situations; and A2. The organization employs automated mechanisms to provide a realistic Smart Grid information system training environment.	SG.IR-3.1 Determine if: (i) personnel are trained in their incident response roles and responsibilities with respect to the Smart Grid information system on an organization-defined frequency; (ii) personnel refresher training on an organization-defined frequency for their incident response roles and responsibilities with respect to the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Incident response policy; procedures addressing incident response training; automated mechanisms supporting incident response training; incident response training material; security plan; incident response plan; incident response training records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident response training and operational responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.IR-4	Incident Response Testing and Exercises	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization tests and/or exercises the incident response capability for the information system at an organization-defined frequency using organization-defined tests and/or exercises to determine the incident response effectiveness and documents the results. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations The organization employs automated mechanisms to more thoroughly and effectively test/exercise the incident response capability	SG.IR-4.1 Determine if: (i) the organization tests and / or exercises the incident response capability for the Smart Grid information system at an organization-defined frequency using organization-defined tests and / or exercises to determine the incident response effectiveness and documents the results; (ii) the organization documents the test and / or exercise results on the incident response capability for the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Incident response policy; procedures addressing incident response testing and exercises; security plan; incident response testing documentation; automated mechanisms supporting incident response tests/exercises; incident response plan; incident response testing material; incident response test results; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident response testing responsibilities].
SG.IR-5	Incident Handling	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, mitigation, and recovery; 2. Integrates incident handling procedures with continuity of operations procedures; and 3. Incorporates lessons learned from incident handling activities into incident response procedures. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization employs automated mechanisms to administer and support the incident handling process.	SG.IR-5.1 Determine if: (i) the organization implements an incident handling capability for security incidents that includes a) preparation b) detection c) analysis d) containment e) mitigation f) recovery; (ii) the organization integrates incident handling procedures with continuity of operations procedures; (iii) the organization incorporates lessons learned from incident handling activities into incident response procedures.	Examine, Interview, Test	Examine: [SELECT FROM: Incident response policy; procedures addressing incident handling; incident response plan; automated mechanisms supporting incident handling; security plan; incident response plan; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident handling responsibilities; organizational personnel with contingency planning responsibilities]. Test: [SELECT FROM: Incident handling capability for the organization].
SG.IR-6	Incident Monitoring	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization tracks and documents Smart Grid information system and network security incidents. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization employs automated mechanisms to assist in the tracking of security incidents and in the collection and analysis of incident information.	SG.IR-6.1 Determine if: (i) the organization tracks Smart Grid information system and network security incidents; (ii) the organization documents Smart Grid information system and network security incidents.	Examine, Interview, Test	Examine: [SELECT FROM: Incident response policy; procedures addressing incident monitoring; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; incident response records and documentation; automated mechanisms supporting incident monitoring; incident response plan; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident monitoring responsibilities]. Test: [SELECT FROM: Incident monitoring capability for the organization; Automated mechanisms assisting in tracking of security incidents and in the collection and analysis of incident information].
SG.IR-7	Incident Reporting	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization incident reporting procedure includes: a. What is a reportable incident; b. The granularity of the information reported; c. Who receives the report; and d. The process for transmitting the incident information. 2. Detailed incident data is reported in a manner that complies with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization employs automated mechanisms to assist in the reporting of security incidents.	SG.IR-7.1 Determine if the organization incident reporting procedure includes: a) What is a reportable incident; b) The granularity of the information reported; c) Who receives the report; and d) The process for transmitting the incident information. SG.IR-7.2 Determine if the organization's detailed incident data is reported in a manner that complies with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Incident response policy; procedures addressing incident reporting; incident reporting records and documentation; security plan; incident response plan; automated mechanisms supporting incident reporting; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with incident reporting responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.IR-8	Incident Response Investigation and Analysis	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization policies and procedures include an incident response investigation and analysis program; 2. The organization includes investigation and analysis of Smart Grid information system incidents in the planning process; and 3. The organization develops, tests, deploys, and documents an incident investigation and analysis process. Supplemental Guidance The organization documents its policies and procedures to show that investigation and analysis of incidents are included in the planning process. The procedures ensure that the Smart Grid information system is capable of providing event data to the proper personnel for analysis and for developing mitigation steps. Requirement Enhancements None. Additional Considerations None.	SG.IR-8.1 Determine if the organization policies and procedures include an incident response investigation and analysis program. SG.IR-8.2 Determine if the organization includes investigation and analysis of Smart Grid information system incidents in the planning process. SG.IR-8.3 Determine if: (i) the organization develops an incident investigation and analysis process; (ii) the organization tests an incident investigation and analysis process; (iii) the organization deploys an incident investigation and analysis process; (iv) the organization documents an incident investigation and analysis process.	Examine, Interview, Test	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; physical intrusion alarm / surveillance equipment logs or records; Smart Grid information system design documentation; security plan; physical access logs or records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with physical access monitoring responsibilities]. Test: [SELECT FROM: Physical access monitoring capability; Automated mechanisms implementing physical access monitoring capability].
SG.IR-9	Corrective Action	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization reviews investigation results and determines corrective actions needed; and 2. The organization includes processes and mechanisms in the planning to ensure that corrective actions identified as the result of cyber security and Smart Grid information system incidents are fully implemented. Supplemental Guidance The organization encourages and promotes cross-industry incident information exchange and cooperation to learn from the experiences of others. Requirement Enhancements None. Additional Considerations	SG.IR-9.1 Determine if the organization reviews investigation results and determines corrective actions needed. SG.IR-9.2 Determine if the organization includes processes and mechanisms in the planning to ensure that corrective actions identified as the result of cyber security and Smart Grid information system incidents are fully implemented.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; physical intrusion alarm / surveillance equipment logs or records; Smart Grid information system design documentation; security plan; physical access logs or records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with physical access monitoring responsibilities].
SG.IR-10	Smart Grid Information System Backup	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Conducts backups of user-level information contained in the Smart Grid information system on an organization-defined frequency; 2. Conducts backups of Smart Grid information system-level information (including Smart Grid information system state information) contained in the Smart Grid information system on an organization-defined frequency; 3. Conducts backups of information system documentation including security-related documentation on an organization-defined frequency consistent with recovery time; and 4. Protects the confidentiality and integrity of backup information at the storage location. Supplemental Guidance The protection of Smart Grid information system backup information while in transit is beyond the scope of this requirement. Requirement Enhancements 1. The organization tests backup information at an organization-defined frequency to verify media reliability and information integrity; 2. The organization selectively uses backup information in the restoration of Smart Grid information system functions as part of continuity of operations testing; and 3. The organization stores backup copies of the operating system and other critical Smart Grid information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.	SG.IR-10.1 Determine if the organization conducts backups of user-level information contained in the Smart Grid information system on an organization-defined frequency. SG.IR-10.2 Determine if the organization conducts backups of Smart Grid information system-level information (including Smart Grid information system state information) contained in the Smart Grid information system on an organization-defined frequency. SG.IR-10.3 Determine if the organization conducts backups of Smart Grid information system documentation including security-related documentation on an organization-defined frequency consistent with recovery time. SG.IR-10.4 Determine if the organization protects the confidentiality and integrity of backup information at the storage location. SG.IR-10.5 (requirement enhancements 1) Determine if the organization tests backup information at an organization-defined frequency to verify media reliability and information integrity. SG.IR-10.6 (requirement enhancements 2) Determine if the organization selectively uses backup information in the restoration of Smart Grid information system functions as part of continuity of operations testing. SG.IR-10.7 (requirement enhancements 3) Determine if the organization stores backup copies of the operating system and other critical Smart Grid information system software in a separate facility or in a fire-rated container that is not collocated with the operational software.	Examine, Interview	Examine: [SELECT FROM: Contingency planning policy; contingency plan; procedures addressing Smart Grid information system backup; Smart Grid information system backup test results; contingency plan test results; contingency plan testing and / or exercise documentation; backup storage location(s); secondary backup storage location(s); redundant secondary system for Smart Grid information system backups; security plan alternate site service agreements; backup storage location(s); Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with contingency planning and plan implementation responsibilities; organizational personnel with Smart Grid information system backup responsibilities].
SG.IR-11	Coordination of Emergency Response	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization's security policies and procedures delineate how the organization implements its emergency response plan and coordinates efforts with law enforcement agencies, regulators, Internet service providers and other relevant organizations in the event of a security incident. Supplemental Guidance The organization expands relationships with local emergency response personnel to include information sharing and coordinated response to cyber security incidents. Requirement Enhancements None. Additional Considerations	SG.IR-10.1 Determine if: (i) the organization's security policies and procedures delineate how the organization implements its emergency response plan; (ii) the organization's security policies and procedures coordinates efforts with law enforcement agencies, regulators, Internet service providers and other relevant organizations in the event of a security incident.	Examine, Interview	Examine: [SELECT FROM: Incident response / emergency management policy; procedures addressing incident response planning; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security configuration responsibilities; organization personnel with incident response planning responsibilities].
Smart Grid Information System Development and Maintenance (SG.MA)						

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented Smart Grid information system maintenance security policy that addresses— i. The objectives, roles, and responsibilities for the Smart Grid information system maintenance security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the Smart Grid information system maintenance security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the Smart Grid information system maintenance security policy and associated Smart Grid information system maintenance protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the Smart Grid information system maintenance security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The Smart Grid information system maintenance policy can be included as part of the general information security policy for the organization. Smart Grid information system maintenance procedures can be developed for the security program in general and for a particular Smart Grid information system when required. Requirement Enhancements	SG.MA-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency— a) A documented Smart Grid information system maintenance security policy that addresses— 1) The objectives, roles, and responsibilities for the Smart Grid information system maintenance security program as it relates to protecting the organization's personnel and assets; and 2) The scope of the Smart Grid information system maintenance security program as it applies to all of the organizational staff, contractors, and third parties; and b) Procedures to address the implementation of the Smart Grid information system maintenance security policy and associated Smart Grid information system maintenance protection requirements. SG.MA-1.2 Determine if: (i) the organization documents management's commitment to ensure compliance with the organization's security policy and other regulatory requirements; (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG.MA-1.3 Determine if the organization ensures that the Smart Grid information system maintenance security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.MA-2	Legacy Smart Grid Information System Updates	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization develops policies and procedures to upgrade existing legacy Smart Grid information systems to include security mitigating measures commensurate with the organization's risk tolerance and the risk to the Smart Grid information system. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations	SG.MA-2.1 Determine if the organization develops policies and procedures to upgrade existing legacy Smart Grid information systems to include security mitigating measures commensurate with the organization's risk tolerance and the risk to the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; procedures addressing security-related activity planning for the Smart Grid information system; Smart Grid information system maintenance policy; procedures addressing controlled maintenance for the Smart Grid information system; maintenance records; manufacturer / vendor maintenance specifications; equipment sanitization records; media sanitization records; automated mechanisms supporting Smart Grid information system maintenance activities; Smart Grid information system configuration settings and associated documentation; maintenance records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security planning and plan implementation responsibilities; Organizational personnel with Smart Grid information system maintenance responsibilities].
SG.MA-3	Smart Grid Information System Maintenance	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Schedules, performs, documents, and reviews records of maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and/or organizational requirements; 2. Explicitly approves the removal of the Smart Grid information system or Smart Grid information system components from organizational facilities for off-site maintenance or repairs; 3. Sanitizes the equipment to remove all critical/sensitive information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; 4. Checks all potentially impacted security requirements to verify that the requirements are still functioning properly following maintenance or repair actions; and 5. Makes and secures backups of critical Smart Grid information system software, applications, and data for use if the operating system becomes corrupted or destroyed. Supplemental Guidance All maintenance activities to include routine, scheduled maintenance and repairs, and unplanned maintenance are controlled whether performed on site or remotely and whether the equipment is serviced on site or removed to another location. Maintenance procedures that require the physical removal of any Smart Grid information system component needs to be documented, listing the date, time, reason for removal, estimated date of reinstallation, and name personnel removing components. Requirement Enhancements 1. The organization maintains maintenance records for the Smart Grid information system that include: a. The date and time of maintenance; b. Name of the individual performing the maintenance; c. Name of escort, if necessary; d. A description of the maintenance performed; and e. A list of equipment removed or replaced (including identification numbers, if applicable). Additional Considerations A1. The organization employs automated mechanisms to schedule and document maintenance and repairs as required, producing up-to-date, accurate, complete, and available records of all maintenance and repair actions needed, in process, and completed.	SG.MA-3.1 Determine if: (i) the organization schedules maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and / or organizational requirements; (ii) the organization performs maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and / or organizational requirements; (iii) the organization documents maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and / or organizational requirements; (iv) the organization reviews records of maintenance and repairs on Smart Grid information system components in accordance with manufacturer or vendor specifications and / or organizational requirements. SG.MA-3.2 Determine if the organization explicitly approves the removal of the Smart Grid information system or Smart Grid information system components from organizational facilities for off-site maintenance or repairs. SG.MA-3.3 Determine if the organization sanitizes the equipment to remove all critical/sensitive information from associated media prior to removal from organizational facilities for off-site maintenance or repairs. SG.MA-3.4 Determine if the organization checks all potentially impacted security requirements to verify that the requirements are still functioning properly following maintenance or repair actions. SG.MA-3.5 Determine if the organization makes and secures backups of critical Smart Grid information system software, applications, and data for use if the operating system becomes corrupted or destroyed. SG.MA-3.6 (requirement enhancement 1) Determine if the organization maintains maintenance records for the Smart Grid information system that include: a) The date and time of maintenance; b) Name of the individual performing the maintenance; c) Name of escort, if necessary; d) A description of the maintenance performed; and e) A list of equipment removed or replaced (including identification numbers, if applicable).	Examine, Interview	Examine: [SELECT FROM: Security planning policy; procedures addressing security-related activity planning for the Smart Grid information system; Smart Grid information system maintenance policy; procedures addressing controlled maintenance for the Smart Grid information system; maintenance records; manufacturer / vendor maintenance specifications; equipment sanitization records; media sanitization records; automated mechanisms supporting Smart Grid information system maintenance activities; Smart Grid information system configuration settings and associated documentation; maintenance records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security planning and plan implementation responsibilities; Organizational personnel with Smart Grid information system maintenance responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.MA-4	Maintenance Tools	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization approves and monitors the use of Smart Grid information system maintenance tools. Supplemental Guidance The requirement addresses security-related issues when the hardware, firmware, and software are brought into the Smart Grid information system for diagnostic and repair actions. Requirement Enhancements None. Additional Considerations A1. The organization requires approval from a management authority explicitly authorizing removal of equipment from the facility; A2. The organization inspects all maintenance tools carried into a facility by maintenance personnel for obvious improper modifications; A3. The organization checks all media containing diagnostic and test programs for malicious code before the media are used in the Smart Grid information system; and A4. The organization employs automated mechanisms to restrict the use of maintenance tools to authorized personnel only.	SG.MA-4.1 Determine if: (i) the organization approves the use of Smart Grid information system maintenance tools; (ii) the organization monitors the use of Smart Grid information system maintenance tools.	Examine, Interview, Test	Examine: [SELECT FROM: Smart Grid information system maintenance policy; Smart Grid information system maintenance tools and associated documentation; procedures addressing Smart Grid information system maintenance tools; automated mechanisms supporting Smart Grid information system maintenance activities; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; maintenance records; Smart Grid information system media containing maintenance programs (including diagnostic and test programs); maintenance records; equipment sanitization records; media sanitization records; exemptions for equipment removal; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system maintenance responsibilities]. Test: [SELECT FROM: Automated mechanisms supporting Smart Grid information system maintenance activities; Media checking process for malicious code detection].
SG.MA-5	Maintenance Personnel	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization documents authorization and approval policies and procedures for maintaining a list of personnel authorized to perform maintenance on the Smart Grid information system; and 2. When maintenance personnel do not have needed access authorizations, organizational personnel with appropriate access authorizations supervise maintenance personnel during the performance of maintenance activities on the Smart Grid information system. Supplemental Guidance Maintenance personnel need to have appropriate access authorization to the Smart Grid information system when maintenance activities allow access to organizational information that could result in a future compromise of availability, integrity, or confidentiality. Requirement Enhancements None. Additional Considerations None.	SG.MA-5.1 Determine if the organization documents authorization and approval policies and procedures for maintaining a list of personnel authorized to perform maintenance on the Smart Grid information system. SG.MA-5.2 Determine if authorized organizational personnel with appropriate maintenance access supervise unauthorized maintenance personnel during the performance of maintenance activities on the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system maintenance policy; procedures addressing maintenance personnel; Smart Grid information system media protection policy; physical and environmental protection policy; security plan; list of maintenance personnel requiring escort / supervision; maintenance records; access control policy and procedures; physical and environmental protection policy and procedures; memorandum of agreement; maintenance records; access control records; service provider contracts and / or service level agreements; list of authorized personnel; maintenance records; maintenance records; access authorizations; access credentials; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system maintenance responsibilities; organizational personnel with personnel security responsibilities; organizational personnel with physical access control responsibilities].
SG.MA-6	Remote Maintenance	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization policy and procedures for remote maintenance include: 1. Authorization and monitoring the use of remote maintenance and diagnostic activities; 2. Use of remote maintenance and diagnostic tools; 3. Maintenance records for remote maintenance and diagnostic activities; 4. Termination of all remote maintenance sessions; and 5. Management of authorization credentials used during remote maintenance. Supplemental Guidance None. Requirement Enhancements The organization— 1. Requires that remote maintenance or diagnostic services be performed from an information system that implements a level of security at least as high as that implemented on the Smart Grid information system being serviced; or 2. Removes the component to be serviced from the Smart Grid information system and prior to remote maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities and after the service is performed, sanitizes the component (with regard to potentially malicious software) before returning the component to the Smart Grid information system. Additional Considerations A1. The organization requires that remote maintenance sessions are protected through the use of a strong authentication credential; and A2. The organization requires that (a) maintenance personnel notify the Smart Grid information system administrator when remote maintenance is planned (e.g., date/time), and (b) a management authority approves the remote maintenance.	SG.MA-6.1 Determine if the organization policy and procedures for remote maintenance include: a) authorization and monitoring the use of remote maintenance and diagnostic activities; b) use of remote maintenance and diagnostic tools; c) maintenance records for remote maintenance and diagnostic activities; d) termination of all remote maintenance sessions; and e) management of authorization credentials used during remote maintenance. SG.MA-6.2 (requirement enhancement 1) Determine if the organization requires that remote maintenance or diagnostic services be performed from a Smart Grid information system that implements a level of security at least as high as that implemented on the Smart Grid information system being serviced. SG.MA-6.3 (requirement enhancement 2) Determine if the organization removes the component to be serviced from the Smart Grid information system and prior to remote maintenance or diagnostic services, sanitizes the component (with regard to organizational information) before removal from organizational facilities and after the service is performed, sanitizes the component (with regard to potentially malicious software) before returning the component to the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system maintenance policy; procedures addressing non-local maintenance for the Smart Grid information system; service provider contracts and / or service level agreements; cryptographic mechanisms supporting Smart Grid information system maintenance activities; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; maintenance records; security plan; audit records; maintenance records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system maintenance responsibilities; Smart Grid information system maintenance provider].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.MA-7	Timely Maintenance	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization obtains maintenance support and spare parts for an organization-defined list of security-critical Smart Grid information system components. Supplemental Guidance The organization specifies those Smart Grid information system components that, when not operational, result in increased risk to organizations or individuals because the security functionality intended by that component is not being provided. Requirement Enhancements None. Additional Considerations None.	SG.MA-7.1 Determine if: (i) the organization obtains maintenance support for an organization-defined list of security-critical Smart Grid information system components; (ii) the organization obtains spare parts for an organization-defined list of security-critical Smart Grid information system components.	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system maintenance policy; procedures addressing timely maintenance for the Smart Grid information system; service provider contracts and / or service level agreements; inventory and availability of spare parts; security plan; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system maintenance responsibilities].
			Media Protection (SG.MP)			
SG.MP-1	Media Protection Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented media protection security policy that addresses— i. The objectives, roles, and responsibilities for the media protection security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the media protection security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the media protection security policy and associated media protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the media protection security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The media protection policy can be included as part of the general security policy for the organization. Media protection procedures can be developed for the security program in general and for a particular Smart Grid information system when required. Requirement Enhancements None. Additional Considerations None.	SG.MP-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency— a) A documented media protection security policy that addresses— 1) The objectives, roles, and responsibilities for the media protection security program as it relates to protecting the organization's personnel and assets; and 2) The scope of the media protection security program as it applies to all of the organizational staff, contractors, and third parties; and b) Procedures to address the implementation of the media protection security policy and associated media protection requirements. SG.MP-1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirement; (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG.MP-1.3 Determine if the organization ensures that the media protection security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.MP-2	Media Sensitivity Level	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The sensitivity level of media indicates the protection required commensurate with the impact of compromise. Supplemental Guidance These media sensitivity levels provide guidance for access and control to include sharing, copying, transmittal, and distribution appropriate for the level of protection required. Requirement Enhancements None. Additional Considerations --	SG.MP-2.1 Determine if: (i) the organization documents the sensitivity levels of media; (ii) the sensitivity level of media indicates the protection required commensurate with the impact of compromise.	Examine, Interview	Examine: [SELECT FROM: Risk assessment policy; procedures addressing security categorization of organizational information and Smart Grid information systems; security planning policy and procedures; security plan; security categorization documentation; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security categorization and risk assessment responsibilities].
SG.MP-3	Media Marking	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization marks removable Smart Grid information system media and Smart Grid information system output in accordance with organization-defined policy and procedures. Supplemental Guidance Smart Grid information system markings refer to the markings employed on external media (e.g., video displays, hardcopy documents output from the Smart Grid information system). External markings are distinguished from internal markings (i.e., the labels used on internal data structures within the Smart Grid information system). Requirement Enhancements None. Additional Considerations	SG.MP-3.1 Determine if: (i) the organization marks removable Smart Grid information system media in accordance with organization-defined policy and procedures; (ii) the organization marks Smart Grid information system output in accordance with organization-defined policy and procedures.	Examine, Interview, Test	Examine: [SELECT FROM: Smart Grid information system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; security plan; removable storage media and Smart Grid information system output; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media protection and marking responsibilities]. Test: [SELECT FROM: Automated mechanisms supporting removable media marking; Media checking process for markings on removable media; Removable media].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.MP-4	Media Storage	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization physically manages and stores Smart Grid information system media within protected areas. The sensitivity of the material determines how the media are stored. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations -	SG.MP-4.1 Determine if: (i) the organization documents the storage requirements of stored media; (ii) the organization physically manages Smart Grid information system media within protected areas; (iii) the organization physically stores Smart Grid information system media within protected areas.	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; procedures addressing media access; access control policy and procedures; physical and environmental protection policy and procedures; media storage facilities; access control devices; access control records; audit records; security plan; Smart Grid information system media; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media protection and storage responsibilities].
SG.MP-5	Media Transport	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Protects organization-defined types of media during transport outside controlled areas using organization-defined security measures; 2. Maintains accountability for Smart Grid information system media during transport outside controlled areas; and 3. Restricts the activities associated with transport of such media to authorized personnel. Supplemental Guidance A controlled area is any space for which the organization has confidence that the physical and procedural protections provided are sufficient to meet the requirements established for protecting the information and Smart Grid information system. Requirement Enhancements None. Additional Considerations A1. The organization employs an identified custodian throughout the transport of Smart Grid information system media; and A2. The organization documents activities associated with the transport of Smart Grid information system media using an organization-defined Smart Grid information system of records.	SG.MP-5.1 Determine if the organization protects organization-defined types of media during transport outside controlled areas using organization-defined security measures. SG.MP-5.2 Determine if the organization maintains accountability for Smart Grid information system media during transport outside controlled areas. SG.MP-5.3 Determine if the organization restricts the activities associated with transport of such media to authorized personnel.	Examine, Interview, Test	Examine: [SELECT FROM: Smart Grid information system media protection policy; procedures addressing media transport; physical and environmental protection policy and procedures; access control policy and procedures; security plan; list of organization-defined personnel authorized to transport Smart Grid information system media outside of controlled areas; Smart Grid information system media; Smart Grid information system media transport records; Smart Grid information system audit records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media transport responsibilities]. Test: [SELECT FROM: Mechanisms protecting information during transportation outside controlled areas].
SG.MP-6	Media Sanitization and Disposal	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization sanitizes Smart Grid information system media before disposal or release for reuse. The organization tests sanitization equipment and procedures to verify correct performance on an organization-defined frequency. Supplemental Guidance Sanitization is the process of removing information from media such that data recovery is not possible. Requirement Enhancements The organization tracks, documents, and verifies media sanitization and disposal actions. Additional Considerations None.	SG.MP-6.1 Determine if: (i) the organization sanitizes Smart Grid information system media before disposal or release for reuse; (ii) the organization tests sanitization equipment and procedures to verify correct performance on an organization-defined frequency. SG.MP-6.2 (requirement enhancement 1) Determine if: (i) the organization tracks media sanitization and disposal actions; (ii) the organization documents media sanitization and disposal actions; (iii) the organization verifies media sanitization and disposal actions.	Examine, Interview	Examine: [SELECT FROM: Smart Grid information system media protection policy; procedures addressing media sanitization and disposal; media sanitization records; audit records; media sanitization equipment test records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system media sanitization responsibilities].
Physical and Environmental Security (SG.PE)						

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.PE-1	Physical and Environmental Security Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented physical and environmental security policy that addresses— i. The objectives, roles, and responsibilities for the physical and environmental security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the physical and environmental security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the physical and environmental security policy and associated physical and environmental protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the physical and environmental security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The organization may include the physical and environmental security policy as part of the general security policy for the organization. Requirement Enhancements None. Additional Considerations None.	SG.PE-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency— a) A documented physical and environmental security policy that addresses— 1) The objectives, roles, and responsibilities for the physical and environmental security program as it relates to protecting the organization's personnel and assets; and 2) The scope of the physical and environmental security program as it applies to all of the organizational staff, contractors, and third parties; and b) Procedures to address the implementation of the physical and environmental security policy and associated physical and environmental protection requirements. SG.PE-1.2 Determine if: (i) the organization documents management commitment to ensure compliance with the organization's security policy and other regulatory requirement; (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG.PE-1.3 Determine if the organization ensures that the physical and environmental security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.PE-2	Physical Access Authorizations	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops and maintains lists of personnel with authorized access to facilities containing Smart Grid information systems and issues appropriate authorization credentials (e.g., badges, identification cards); and 2. Designated officials within the organization review and approve access lists on an organization-defined frequency, removing from the access lists personnel no longer requiring access. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization authorizes physical access to the facility where the Smart Grid information system resides based on position or role; A2. The organization requires multiple forms of identification to gain access to the facility where the Smart Grid information system resides; and A3. The organization requires multifactor authentication to gain access to the facility where the Smart Grid information system resides.	SG.PE-2.1 Determine if: (i) the organization develops lists of personnel with authorized access to facilities containing Smart Grid information systems; (ii) the organization maintains lists of personnel with authorized access to facilities containing Smart Grid information systems; (iii) the organization issues appropriate authorization credential to personnel for facilities containing Smart Grid information systems. SG.PE-2.2 Determine if: (i) the organization documents designated officials to review and approval access lists for authorization credential to personnel for facilities containing Smart Grid information systems; (ii) designated officials within the organization review, update and approve access lists on an organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access authorizations; security plan; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; physical access control logs or records; Smart Grid information system entry and exit points; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to Smart Grid information system facility].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.PE-3	Physical Access	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Enforces physical access authorizations for all physical access points to the facility where the Smart Grid information system resides; 2. Verifies individual access authorizations before granting access to the facility; 3. Controls entry to facilities containing Smart Grid information systems; 4. Secures keys, combinations, and other physical access devices; 5. Inventories physical access devices on a periodic basis; and 6. Changes combinations, keys, and authorization credentials on an organization-defined frequency and when keys are lost, combinations are compromised, individual credentials are lost, or individuals are transferred or terminated. Supplemental Guidance Physical access devices include keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) an organizational Smart Grid information system may be located in areas designated as publicly accessible with access to such devices being safeguarded. Requirement Enhancements 1. The organization requires physical access mechanisms to Smart Grid information system assets in addition to physical access mechanisms to the facility; and 2. The organization employs hardware to deter unauthorized physical access to Smart Grid information system devices. Additional Considerations A1. The organization ensures that every physical access point to the facility where the Smart Grid information system resides is guarded or alarmed and monitored on an organization-defined frequency.	SG.PE-3.1 Determine if: (i) the organization documents all physical access authorizations for all physical access points to the facility where the Smart Grid information system resides; (ii) the organization enforces physical access authorizations for all physical access points to the facility where the Smart Grid information system resides. SG.PE-3.2 Determine if the organization verifies individual access authorizations before granting access to the facility. SG.PE-3.3 Determine if the organization controls entry to facilities containing Smart Grid information systems. SG.PE-3.4 Determine if the organization secures keys, combinations, and other physical access devices. SG.PE-3.5 Determine if the organization inventories physical access devices on a periodic basis. SG.PE-3.6 Determine if: (i) the organization changes combinations, keys, and authorization credentials on an organization-defined frequency; (ii) the organization changes combinations, keys, and authorization credentials when a) keys are lost b) combinations are compromised c) individual credentials are lost d) individuals are transferred e) individuals are terminated. SG.PE-3.7 (requirement enhancement 1) Determine if the organization requires physical access mechanisms to Smart Grid information system assets in addition to physical access mechanisms to the facility. SG.PE-3.8 (requirement enhancement 2) Determine if the organization employs hardware to deter unauthorized physical access to Smart Grid information system devices.	Examine, Interview, Test	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing access control for display medium; facility surveillance records; records of security checks; physical access control logs or records; inventory records of physical access devices; records of key and lock combination changes; storage locations for physical access devices; facility layout documentation; Smart Grid information system entry and exit points; list of Smart Grid information system components requiring protection through lockable physical casings; lockable physical casings; facility layout of Smart Grid information system components; actual displays from Smart Grid information system components; Smart Grid information system design documentation; facility communications and wiring diagrams; procedures addressing physical access control; physical access control logs or records; procedures addressing penetration testing; rules of engagement and associated documentation; penetration test results; security plan; list of areas within the facility containing high concentrations of Smart Grid information system components or Smart Grid information system components requiring additional physical protection; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with physical access control responsibilities]. Test: [SELECT FROM: Physical access control capability; physical access control devices].
SG.PE-4	Monitoring Physical Access	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Monitors physical access to the Smart Grid information system to detect and respond to physical security incidents; 2. Reviews physical access logs on an organization-defined frequency; 3. Coordinates results of reviews and investigations with the organization's incident response capability; and 4. Ensures that investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization installs and monitors real-time physical intrusion alarms and surveillance equipment; and A2. The organization implements automated mechanisms to recognize potential intrusions and initiates designated response actions.	SG.PE-4.1 Determine if the organization monitors physical access to the Smart Grid information system to detect and respond to physical security incidents. SG.PE-4.2 Determine if: (i) the organization logs physical access to the Smart Grid information system; (ii) the organization reviews physical access logs on an organization-defined frequency. SG.PE-4.3 Determine if: (i) the organization coordinates results of reviews with the organization's incident response capability; (ii) the organization coordinates results of investigations with the organization's incident response capability. SG.PE-4.4 Determine if the organization ensures that investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability.	Examine, Interview, Test	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing physical access monitoring; security plan; physical intrusion alarm / surveillance equipment logs or records; physical access logs or records; Smart Grid information system design documentation; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with physical access monitoring responsibilities]. Test: [SELECT FROM: Physical access monitoring capability; Automated mechanisms implementing physical access monitoring capability].
SG.PE-5	Visitor Control	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization controls physical access to the Smart Grid information system by authenticating visitors before authorizing access to the facility. Supplemental Guidance Contractors and others with permanent authorization credentials are not considered visitors. Requirement Enhancements The organization escorts visitors and monitors visitor activity as required according to security policies and procedures. Additional Considerations A1. The organization requires multiple forms of identification for access to the facility.	SG.PE-5.1 Determine if: (i) the organization documents physical access to the Smart Grid information system; (ii) the organization controls physical access to the Smart Grid information system by authenticating visitors before authorizing access to the facility. SG.PE-5.2 (requirement enhancement 1) Determine if: (i) the organization documents that visitors are escorted and required to adhere to the organization's security policies and procedures; (ii) the organization escorts visitors as required according to security policies and procedures; (iii) the organization monitors visitor activity as required according to security policies and procedures.	Examine, Interview, Test	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing visitor access control; visitor access control logs or records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with visitor access control responsibilities]. Test: [SELECT FROM: Visitor access control capability].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.PE-6	Visitor Records	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization maintains visitor access records to the facility that include: 1. Name and organization of the person visiting; 2. Signature of the visitor; 3. Form of identification; 4. Date of access; 5. Time of entry and departure; 6. Purpose of visit; and 7. Name and organization of person visited. Designated officials within the organization review the access logs after closeout and periodically review access logs based on an organization-defined frequency. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization employs automated mechanisms to facilitate the maintenance and review of access records.	SG.PE-6.1 Determine if: (i) the organization maintains visitor access records to the facility that include: a) Name and organization of the person visiting; b) Signature of the visitor; c) Form of identification; d) Date of access; e) Time of entry and departure; f) Purpose of visit; and g) Name and organization of person visited. (ii) the organization documents designated officials within the organization to review the access logs after closeout and periodically review access logs based on an organization-defined frequency; (iii) designated officials within the organization to review the access logs after closeout and periodically review access logs based on an organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; automated mechanisms supporting management of access records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for reviewing physical access records].
SG.PE-7	Physical Access Log Retention	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization retains all physical access logs for as long as dictated by any applicable regulations or based on an organization-defined period by approved policy. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations	SG.PE-7.1 Determine if the organization retains all physical access logs for as long as dictated by any applicable regulations or based on an organization-defined period by approved policy.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing facility access records; security plan; facility access control records; automated mechanisms supporting management of access records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for reviewing physical access records].
SG.PE-8	Emergency Shutoff Protection	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization protects the emergency power-off capability from accidental and intentional/unauthorized activation. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations None.	SG.PE-8.1 Determine if the organization protects the emergency power-off capability from accidental and intentional/unauthorized activation.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing power source emergency shutoff; security plan; emergency shutoff controls or switches; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to Smart Grid information system facility].
SG.PE-9	Emergency Power	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization provides an alternate power supply to facilitate an orderly shutdown of noncritical Smart Grid information system components in the event of a primary power source loss. Supplemental Guidance None. Requirement Enhancements 1. The organization provides a long-term alternate power supply for the Smart Grid information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source. Additional Considerations A1. The organization provides a long-term alternate power supply for the Smart Grid information system that is self-contained and not reliant on external power generation.	SG.PE-9.1 Determine if the organization provides an alternate power supply to facilitate an orderly shutdown of noncritical Smart Grid information system components in the event of a primary power source loss. SG.PE-9.2 (requirement enhancement 1) Determine if the organization provides a long-term alternate power supply for the Smart Grid information system that is capable of maintaining minimally required operational capability in the event of an extended loss of the primary power source.	Examine, Interview, Test	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing emergency power; uninterruptible power supply documentation; uninterruptible power supply test records; alternate power supply documentation; alternate power test records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with physical access authorization responsibilities; organizational personnel with physical access to Smart Grid information system facility]. Test: [SELECT FROM: Uninterruptible power supply; Alternate power supply].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.PE-10	Delivery and Removal	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization authorizes, monitors, and controls organization-defined types of Smart Grid information system components entering and exiting the facility and maintains records of those items. Supplemental Guidance The organization secures delivery areas and, if possible, isolates delivery areas from the Smart Grid information system to avoid unauthorized physical access. Requirement Enhancements None. Additional Considerations	SG.PE-10.1 Determine if: (i) the organization authorizes organization-defined types of Smart Grid information system components entering and exiting the facility and maintains records of those items; (ii) the organization monitors organization-defined types of Smart Grid information system components entering and exiting the facility and maintains records of those items; (iii) the organization controls organization-defined types of Smart Grid information system components entering and exiting the facility and maintains records of those items.	Examine, Interview, Test	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing delivery and removal of Smart Grid information system components from the facility; security plan; facility housing the Smart Grid information system; records of items entering and exiting the facility; other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with responsibilities for controlling Smart Grid information system components entering and exiting the facility]. Test: [SELECT FROM: Process for controlling Smart Grid information system-related items entering and exiting the facility].
SG.PE-11	Alternate Work Site	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization establishes an alternate work site (for example, private residences) with proper equipment and communication infrastructure to compensate for the loss of the primary work site; and 2. The organization implements appropriate management, operational, and technical security measures at alternate control centers. Supplemental Guidance The organization may define different sets of security requirements for specific alternate work sites or types of sites. Requirement Enhancements None. Additional Considerations A1. The organization provides methods for employees to communicate with Smart Grid information system security staff in case of security problems.	SG.PE-11.1 Determine if the organization establishes an alternate work site (for example, private residences) with proper equipment and communication infrastructure to compensate for the loss of the primary work site. SG.PE-11.2 Determine if: (i) the organization implements appropriate management security measures at alternate control centers; (ii) the organization implements appropriate operational security measures at alternate control centers; (iii) the organization implements appropriate technical security measures at alternate control centers.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing alternate work sites for organizational personnel; security plan; list of management, operational, and technical security controls required for alternate work sites; assessments of security controls at alternate work sites; other relevant documents or records]. Interview: [SELECT FROM: Organization personnel using alternate work sites].
SG.PE-12	Location of Smart Grid Information System Assets	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization locates Smart Grid information system assets to minimize potential damage from physical and environmental hazards. Supplemental Guidance Physical and environmental hazards include flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electrical interference, and electromagnetic radiation. Requirement Enhancements 1. The organization considers the risk associated with physical and environmental hazards when planning new Smart Grid information system facilities or reviewing existing facilities. Additional Considerations	SG.PE-12.1 Determine if the organization locates Smart Grid information system assets to minimize potential damage from physical and environmental hazards. SG.PG-12.2 (requirement enhancement 1) Determine if the organization considers the risk associated with physical and environmental hazards when planning new Smart Grid information system facilities or reviewing existing facilities.	Examine, Interview	Examine: [SELECT FROM: Physical and environmental protection policy; procedures addressing positioning of Smart Grid information system components; documentation providing the location and position of Smart Grid information system components within the facility; physical site planning documents; organizational assessment of risk, contingency plan; other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with site selection responsibilities for the facility housing the Smart Grid information system].
Planning (SG.PL)						

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.PL-1	Strategic Planning Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented planning policy that addresses— i. The objectives, roles, and responsibilities for the planning program as it relates to protecting the organization's personnel and assets; and ii. The scope of the planning program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the planning policy and associated strategic planning requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the planning policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The strategic planning policy may be included as part of the general information security policy for the organization. Strategic planning procedures may be developed for the security program in general and a Smart Grid information system in particular, when required. Requirement Enhancements None. Additional Considerations None.	SG.PL-1.1 Determine if: (i) the organization develops a documented security strategic planning policy; (ii) the security strategic planning policy addresses security strategic planning as it related to protecting the organization's personnel and assets and the following: a) purpose / objective b) scope c) roles and responsibilities d) coordination among organizational entities, and compliance; (iii) the security strategic planning policy addresses the scope to include all organizational staff, contractors, and third parties; (iv) the organization implements the security strategic planning procedures; (v) the organization reviews and updates the security strategic planning procedures on an organizational defined frequency. SG.PL-1.2 Determine if: (i) the organization documents management's commitment to ensure compliance with the organization's security strategic planning; (ii) management commitment ensures compliance with the organization's security strategic planning. SG.PL-1.3 Determine if: (i) the security strategic planning policy comply with applicable federal, state, local, tribal, and territorial laws and regulations; and (ii) the security strategic planning procedures facilitate implementation of the security strategic planning security policy. SG.PL-1.4 Determine if: (i) the organization defines the frequency of security strategic planning policy and procedures reviews/updates; (ii) the organization reviews/updates the security strategic planning policy and procedures in accordance with the organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.PL-2	Smart Grid Information System Security Plan	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Develops a security plan for each Smart Grid information system that— a. Aligns with the organization's enterprise architecture; b. Explicitly defines the components of the Smart Grid information system; c. Describes relationships with and interconnections to other Smart Grid information systems; d. Provides an overview of the security objectives for the Smart Grid information system; e. Describes the security requirements in place or planned for meeting those requirements; and f. Is reviewed and approved by the management authority prior to plan implementation; 2. Reviews the security plan for the Smart Grid information system on an organization-defined frequency; and 3. Revises the plan to address changes to the Smart Grid information system/environment of operation or problems identified during plan implementation or security requirement assessments. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations	SG.PL-2.1 Determine if the organization develops a security plan for each Smart Grid information system that a) Aligns with the organization's enterprise architecture; b) Explicitly defines the components of the Smart Grid information system; c) Describes relationships with and interconnections to other Smart Grid information systems; d) Provides an overview of the security objectives for the Smart Grid information system; e) Describes the security requirements in place or planned for meeting those requirements; and f) Is reviewed and approved by the management authority prior to plan implementation. SG.PL-2.2 Determine if the organization reviews the security plan for the Smart Grid information system on an organization-defined frequency. SG.PL-2.3 Determine if the organization revises the plan to address changes to the Smart Grid information system/environment of operation or problems identified during plan implementation or security requirement assessments.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; procedures addressing security plan development and implementation; procedures addressing security plan reviews and updates; enterprise architecture documentation; security plan for the Smart Grid information system; records of security plan reviews and updates; access control policy; contingency planning policy; other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with security planning and plan implementation responsibilities for the Smart Grid information system].
SG.PL-3	Rules of Behavior	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization establishes and makes readily available to all Smart Grid information system users, a set of rules that describes their responsibilities and expected behavior with regard to Smart Grid information system usage. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization includes in the rules of behavior, explicit restrictions on the use of social networking sites, posting information on commercial Web sites, and sharing Smart Grid information system account information; and A2. The organization obtains signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior before authorizing access to the Smart Grid information system.	SG.PL-3.1 Determine if: (i) the organization establishes a set of rules that describe user responsibilities and expected behavior with regard to Smart Grid information system usage, which includes a) use of social networking sites b) posting information on commercial websites c) sharing of Smart Grid information system account information (ii) the organization make readily available a set of rules that describe user responsibilities and expected behavior with regard to Smart Grid information system usage; (iii) the organization receives a signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; procedures addressing rules of behavior for Smart Grid information system users; rules of behavior; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel who are authorized users of the Smart Grid information system and have signed rules of behavior].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.PL-4	Privacy Impact Assessment	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization conducts a privacy impact assessment on the Smart Grid information system; and 2. The privacy impact assessment is reviewed and approved by a management authority. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations -	SG.PL-4.1 Determine if the organization conducts a privacy impact assessment on Smart Grid information systems. SG.PL-4.2 Determine if: (i) the privacy impact assessment is reviewed by an organizational management authority; (ii) the privacy impact assessment is approved by an organizational management authority.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; procedures addressing privacy impact assessments on the Smart Grid information system; privacy impact assessment; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel who have privacy responsibilities].
SG.PL-5	Security-Related Activity Planning	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization plans and coordinates security-related activities affecting the Smart Grid information system before conducting such activities to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, or individuals; and 2. Organizational planning and coordination includes both emergency and nonemergency (e.g., routine) situations. Supplemental Guidance Routine security-related activities include, but are not limited to, security assessments, audits, Smart Grid information system hardware, firmware, and software maintenance, and testing/exercises. Requirement Enhancements None. Additional Considerations	SG.PL-5.1 Determine if: (i) the organization plans security-related activities affecting the Smart Grid information system before conducting such activities to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, or individuals; (ii) the organization coordinates security-related activities affecting the Smart Grid information system before conducting such activities to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, or individuals. SG.PL-5.1 Determine if the organizational planning and coordination includes both emergency and nonemergency (e.g., routine) situations.	Examine, Interview	Examine: [SELECT FROM: Security planning policy; procedures addressing security-related activity planning for the Smart Grid information system; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security planning and plan implementation responsibilities].
			Security Program Management (SG.PM)			
SG.PM-1	Security Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented security program security policy that addresses— i. The objectives, roles, and responsibilities for the security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the security program security policy and associated security program protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the security program security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The information system security policy can be included as part of the general security policy for the organization. Procedures can be developed for the security program in general and for the information system in particular, when required. Requirement Enhancements None. Additional Considerations None.	SG.PM-1.1 Determine if: (i) the organization develops and documents policy and procedure for the security management program; (ii) the organization implements policy and procedure for the security management program; (iii) the organization disseminates policy and procedure to appropriate elements within the organization for the security management program; (iv) the organization reviews the policy and procedure for the security management program on a defined frequency; (v) the security management program policy and procedures address a) purpose b) scope c) roles and responsibilities d) management commitment e) coordination among organizational entities, and compliance. SG.PM-1.2 Determine if: (i) the organization documents management's commitment ensures compliance with the organization's security policy and other regulatory requirements; (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG.PM-1.3 Determine if the organization ensures that the security program security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.PM-2	Security Program Plan	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops and disseminates an organization-wide security program plan that— a. Provides an overview of the requirements for the security program and a description of the security program management requirements in place or planned for meeting those program requirements; b. Provides sufficient information about the program management requirements to enable an implementation that is compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; c. Includes roles, responsibilities, management accountability, coordination among organizational entities, and compliance; and d. Is approved by a management authority with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, and individuals; 2. Reviews the organization-wide security program plan on an organization-defined frequency; and 3. Revises the plan to address organizational changes and problems identified during plan implementation or security requirement assessments. Supplemental Guidance The security program plan documents the organization-wide program management requirements. The security plans for individual information systems and the organization-wide security program plan together, provide complete coverage for all security requirements employed within the organization. Requirement Enhancements None.	SG.PM-2.1 Determine if the organization develops and disseminates an organization-wide security program plan that— a) Provides an overview of the requirements for the security program and a description of the security program management requirements in place or planned for meeting those program requirements; b) Provides sufficient information about the program management requirements to enable an implementation that is compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended; c) Includes roles, responsibilities, management accountability, coordination among organizational entities, and compliance; and d) Is approved by a management authority with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, and individuals. SG.PM-2.2 Determine if the organization reviews the organization-wide security program plan on an organization-defined frequency. SG.PM-2.3 Determine if the organization revises the plan to address organizational changes and problems identified during plan implementation or security requirement assessments.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; procedures addressing information security program plan development and implementation; procedures addressing information security program plan reviews and updates; information security program plan; program management controls documentation; common controls documentation; records of information security program plan reviews and updates; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security planning and plan implementation responsibilities for the information security program].
SG.PM-3	Senior Management Authority	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization appoints a senior management authority with the responsibility for the mission and resources to coordinate, develop, implement, and maintain an organization-wide security program. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations	SG.PM-3.1 Determine if the organization appoints a senior management authority with the responsibility for the mission and resources to coordinate, develop, implement, and maintain an organization-wide security program.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; information security program plan; documentation addressing roles and responsibilities of the senior information security officer position; information security program mission statement; other relevant documents or records]. Interview: [SELECT FROM: Organizational person appointed to the senior information security officer position].
SG.PM-4	Security Architecture	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization develops a security architecture with consideration for the resulting risk to organizational operations, organizational assets, individuals, and other organizations. Supplemental Guidance The integration of security requirements into the organization's enterprise architecture helps to ensure that security considerations are addressed by organizations early in the information system development life cycle. Requirement Enhancements None. Additional Considerations	SG.PM-4.1 Determine if the organization develops security architecture with consideration for the resulting risk to a) organizational operations b) organizational assets c) individuals d) other organizations.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; enterprise architecture policy; procedures addressing information security-related aspects of enterprise architecture development; system development life cycle documentation; enterprise architecture documentation; enterprise security architecture documentation; other relevant documents or records]. Interview: [SELECT FROM: Organizational person appointed to the senior information security officer position].
SG.PM-5	Risk Management Strategy	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Develops a comprehensive strategy to manage risk to organizational operations and assets, individuals, and other organizations associated with the operation and use of information systems; and 2. Implements that strategy consistently across the organization. Supplemental Guidance An organization-wide risk management strategy should include a specification of the risk tolerance of the organization, guidance on acceptable risk assessment methodologies, and a process for consistently evaluating risk across the organization. Requirement Enhancements None. Additional Considerations None.	SG.PM-5.1 Determine if the organization develops a comprehensive strategy to manage Smart Grid information system operational and usage risk to a) organizational operations b) organizational assets c) individuals d) other organizations. SG.PM-5.2 Determine if the organization implements that comprehensive risk strategy consistently across the organization.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; risk management policy; procedures addressing risk management strategy development and implementation; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with risk management strategy development and implementation responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.PM-6	Security Authorization to Operate Process	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Manages (e.g., documents, tracks, and reports) the security state of organizational information systems through security authorization processes; and 2. Fully integrates the security authorization to operate processes into an organization-wide risk management strategy. Supplemental Guidance None. Requirement Enhancements None.	SG.PM-6.1 Determine if the organization manages (e.g., documents, tracks, and reports) the security state of organizational Smart Grid information systems through security authorization processes. SG.PM-6.2 Determine if the organization fully integrates the security authorization to operate processes into an organization-wide risk management strategy.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; security assessment and authorization policy; risk management policy; procedures addressing security authorization processes; security authorization package (including security plan, security assessment report, plan of action and milestones, authorization statement); other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security authorization responsibilities for Smart Grid information systems; organizational personnel with risk management responsibilities].
SG.PM-7	Mission/Business Process Definition	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization defines mission/business processes that include consideration for security and the resulting risk to organizational operations, organizational assets, and individuals. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations	SG.PM-7.1 Determine if the organization defines mission / business processes that include a) consideration for security organizational operations, organizational assets, and individuals; b) the resulting risk to organizational operations, organizational assets, and individuals.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; risk management policy; procedures addressing security categorization of organizational information and Smart Grid information systems; organizational mission / business processes; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with mission / business process definition responsibilities; organizational personnel with security categorization and risk management responsibilities for the information security program].
SG.PM-8	Management Accountability	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization defines a framework of management accountability that establishes roles and responsibilities to approve cyber security policy, assign security roles, and coordinate the implementation of cyber security across the organization. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations None.	SG.PM-8.1 Determine if the organization defines a framework of management accountability that establishes roles and responsibilities to a) approve cyber security policy b) assign security roles c) coordinate the implementation of cyber security across the organization.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; procedures addressing information security program plan development and implementation; procedures addressing information security program plan reviews and updates; information security program plan; program management controls documentation; common controls documentation; records of information security program plan reviews and updates; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security planning and plan implementation responsibilities for the information security program].
			Personnel Security (SG.PS)			
SG.PS-1	Personnel Security Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented personnel security policy that addresses— i. The objectives, roles, and responsibilities for the personnel security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the personnel security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the personnel security policy and associated personnel protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the personnel security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The personnel security policy may be included as part of the general information security policy for the organization. Personnel security procedures can be developed for the security program in general and for a particular Smart Grid information system, when required. Requirement Enhancements None. Additional Considerations None.	SG.PS-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency a) A documented personnel security policy that addresses— 1) The objectives, roles, and responsibilities for the personnel security program as it relates to protecting the organization's personnel and assets; and 2) The scope of the personnel security program as it applies to all of the organizational staff, contractors, and third parties; and b) Procedures to address the implementation of the personnel security policy and associated personnel protection requirements. SG.PS-1.2 Determine if: (i) the organization documents management commitment ensures compliance with the organization's security policy and other regulatory requirements; (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG.PS-1.3 Determine if the organization ensures that the personnel security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.PS-2	Position Categorization	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization assigns a risk designation to all positions and establishes screening criteria for individuals filling those positions. The organization reviews and revises position risk designations. The organization determines the frequency of the review based on the organization's requirements or regulatory commitments. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations --	SG.PS-2.1 Determine if: (i) the organization assigns a risk designation to all positions; (ii) the organization establishes screening criteria for individuals filling designated risk positions; (iii) the organization reviews position risk designations; (iv) the organization revises position risk designations; (v) the organization determines the frequency of the review based on the organization's requirements or regulatory commitments.	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing position categorization; appropriate codes of federal regulations; list of risk designations for organizational positions; security plan; records of risk designation reviews and updates; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].
SG.PS-3	Personnel Screening	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization screens individuals requiring access to the Smart Grid information system before access is authorized. The organization maintains consistency between the screening process and organization-defined policy, regulations, guidance, and the criteria established for the risk designation of the assigned position. Supplemental Guidance Basic screening requirements should include: 1. Employment history; 2. Verification of the highest education degree received; 3. Residency; 4. References; and 5. Law enforcement records. Requirement Enhancements None. Additional Considerations A1. The organization rescreens individuals with access to Smart Grid information systems based on a defined list of conditions requiring rescreening and the frequency of such rescreening.	SG.PS-3.1 Determine if: (i) the organization screens individuals requiring access to the Smart Grid information system before access is authorized; (ii) the organization maintains consistency between the screening process and organization-defined policy, regulations, guidance, and the criteria established for the risk designation of the assigned position.	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel screening; records of screened personnel; security plan; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].
SG.PS-4	Personnel Termination	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. When an employee is terminated, the organization revokes logical and physical access to facilities and systems and ensures that all organization-owned property is returned. Organization-owned documents relating to the Smart Grid information system that are in the employee's possession are transferred to the new authorized owner; 2. All logical and physical access must be terminated at an organization-defined time frame for personnel terminated for cause; and 3. Exit interviews ensure that individuals understand any security constraints imposed by being a former employee and that proper accountability is achieved for all Smart Grid information system-related property. Supplemental Guidance Organization-owned property includes Smart Grid information system administration manuals, keys, identification cards, building passes, computers, cell phones, and personal data assistants. Organization-owned documents include field device configuration and operational information and Smart Grid information system network documentation. Requirement Enhancements None. Additional Considerations A1. The organization implements automated processes to revoke access permissions that are initiated by the termination.	SG.PS-4.1 Determine if: (i) the organization revokes logical and physical access to facilities and systems when an employee is terminated; (ii) the organization ensures that all organization-owned property is returned when an employee is terminated; (iii) the organization-owned documents relating to the Smart Grid information system that are in the employee's possession are transferred to the new authorized owner. SG.PS-4.2 Determine if the organization's logical and physical access must be terminated at an organization-defined time frame for personnel terminated for cause. SG.PS-4.3 Determine if the organization ensures that during the individuals exit interview they understand any security constraints imposed by being a former employee and that proper accountability is achieved for all Smart Grid information system-related property.	Examine, Interview, Test	Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of Smart Grid information system accounts; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.PS-5	Personnel Transfer	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization reviews logical and physical access permissions to Smart Grid information systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions; and 2. Complete execution of this requirement occurs within an organization-defined time period for employees, contractors, or third parties who no longer need to access Smart Grid information system resources. Supplemental Guidance Appropriate actions may include: 1. Returning old and issuing new keys, identification cards, and building passes; 2. Closing old accounts and establishing new accounts; 3. Changing Smart Grid information system access authorizations; and 4. Providing access to official records created or managed by the employee at the former work location and in the former accounts. Requirement Enhancements None. Additional Considerations None.	SG.PS-5.1 Determine if: (i) the organization reviews logical access permissions to Smart Grid information systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions; (ii) the organization reviews physical access permissions to Smart Grid information systems and facilities when individuals are reassigned or transferred to other positions within the organization and initiates appropriate actions. SG.PS-5.2 Determine if: (i) the organization completes the logical access permission review within an organization-defined time period for employees, contractors, or third parties who no longer need to access Smart Grid information system resources; (ii) the organization completes the physical access permission review within an organization-defined time period for employees, contractors, or third parties who no longer need to access Smart Grid information system resources.	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel transfer; security plan; records of personnel transfer actions; list of Smart Grid information system and facility access authorizations; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].
SG.PS-6	Access Agreements	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization completes appropriate agreements for Smart Grid information system access before access is granted. This requirement applies to all parties, including third parties and contractors, who require access to the Smart Grid information system; 2. The organization reviews and updates access agreements periodically; and 3. Signed access agreements include an acknowledgment that individuals have read, understand, and agree to abide by the constraints associated with the Smart Grid information system to which access is authorized. Supplemental Guidance Access agreements include nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Requirement Enhancements None. Additional Considerations	SG.PS-6.1 Determine if: (i) the organization completes appropriate agreements for Smart Grid information system access before access is granted; (ii) the organization ensures the Smart Grid information system access agreements apply to all parties, including third parties and contractors, who require access to the Smart Grid information system. SG.PS-6.2 Determine if: (i) the organization reviews Smart Grid information system access agreements periodically; (ii) the organization updates Smart Grid information system access agreements periodically. SG.PS-6.3 Determine if the organization requires the signed access agreements include an acknowledgment that individuals have read, understand, and agree to abide by the constraints associated with the Smart Grid information system to which access is authorized.	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing access agreements for organizational information and Smart Grid information systems; security plan; access agreements; records of access agreement reviews and updates; signed nondisclosure agreements; personnel security criteria; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].
SG.PS-7	Contractor and Third-Party Personnel Security	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization enforces security requirements for contractor and third-party personnel and monitors service provider behavior and compliance. Supplemental Guidance Contactors and third-party providers include service bureaus and other organizations providing Smart Grid information system operation and maintenance, development, IT services, outsourced applications, and network and security management. Requirement Enhancements None. Additional Considerations None.	SG.PS-7.1 Determine if: (i) the organization enforces Smart Grid information system security requirements for contractor and third-party personnel; (ii) the organization monitors service provider behavior and compliance to Smart Grid information system security requirements.	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing third-party personnel security; list of personnel security requirements; acquisition documents; compliance monitoring process; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities; third-party providers].
SG.PS-8	Personnel Accountability	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization employs a formal accountability process for personnel failing to comply with established security policies and procedures and identifies disciplinary actions for failing to comply; and 2. The organization ensures that the accountability process complies with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The accountability process can be included as part of the organization's general personnel policies and procedures. Requirement Enhancements None. Additional Considerations None.	SG.PS-8.1 Determine if the organization employs a formal accountability process for personnel failing to comply with established security policies and procedures and identifies disciplinary actions for failing to comply. SG.PS-8.2 Determine if the organization ensures that the accountability process complies with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel sanctions; rules of behavior; records of formal sanctions; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.PS-9	Personnel Roles	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization provides employees, contractors, and third parties with expectations of conduct, duties, terms and conditions of employment, legal rights, and responsibilities. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. Employees and contractors acknowledge understanding by signature.	SG.PS-9.1 Determine if the organization provides employees, contractors, and third parties with expectations of conduct, duties, terms and conditions of employment, legal rights, and responsibilities.	Examine, Interview	Examine: [SELECT FROM: Personnel security policy; procedures addressing personnel sanctions; third party policy; third party standards and procedures; rules of behavior; records of formal sanctions; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities; Organizational personnel with third party security responsibilities].
Risk Management and Assessment (SG.RA)						
SG.RA-1	Risk Assessment Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented risk assessment security policy that addresses— i. The objectives, roles, and responsibilities for the risk assessment security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the risk assessment security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the risk assessment security policy and associated risk assessment protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the risk assessment policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The risk assessment policy also takes into account the organization's risk tolerance level. The risk assessment policy can be included as part of the general security policy for the organization. Risk assessment procedures can be developed for the security program in general and for a particular Smart Grid information system, when required. Requirement Enhancements None.	SG.RA-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency a) A documented risk assessment security policy that addresses 1) The objectives, roles, and responsibilities for the risk assessment security program as it relates to protecting the organization's personnel and assets; and 2) The scope of the risk assessment security program as it applies to all of the organizational staff, contractors, and third parties; and b) Procedures to address the implementation of the risk assessment security policy and associated risk assessment protection requirements. SG.RA-1.2 Determine if: (i) the organization documents management commitment ensures compliance with the organization's security policy and other regulatory requirements; (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG.RA-1.3 Determine if the organization ensures that the risk assessment policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.RA-2	Risk Management Plan	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops a risk management plan; 2. A management authority reviews and approves the risk management plan; and 3. Risk-reduction mitigation measures are planned and implemented and the results monitored to ensure effectiveness of the organization's risk management plan. Supplemental Guidance Risk mitigation measures need to be implemented and the results monitored against planned metrics to ensure the effectiveness of the risk management plan. Requirement Enhancements None. Additional Considerations	SG.RA-2.1 Determine if the organization develops a risk management plan. SG.RA-2.2 Determine if: (i) the organization assigns a management authority to review and approve a risk management plan; (ii) a management authority reviews and approves the risk management plan. SG.RA-2.3 Determine if: (i) the organization's risk-reduction mitigation measures are planned to ensure effectiveness of the organization's risk management plan; (ii) the organization's risk-reduction mitigation measures are implemented to ensure effectiveness of the organization's risk management plan; (iii) the organization's risk-reduction mitigation results are monitored to ensure effectiveness of the organization's risk management plan.	Examine, Interview	Examine: [SELECT FROM: Information security program policy; risk management policy; procedures addressing risk management strategy development and implementation; risk management strategy (including risk identification, assessment, mitigation, acceptance, and monitoring methodologies); other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with risk management strategy development and implementation responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.RA-3	Security Impact Level	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Specifies the information and the information system impact levels; 2. Documents the impact level results (including supporting rationale) in the security plan for the information system; and 3. Reviews the Smart Grid information system and information impact levels on an organization-defined frequency. Supplemental Guidance Impact level designation is based on the need, priority, and level of protection required commensurate with sensitivity and impact of the loss of availability, integrity, or confidentiality. Impact level designation may also be based on regulatory requirements, for example, the NERC CIPs. The organization considers safety issues in determining the impact level for the Smart Grid information system. Requirement Enhancements None. Additional Considerations None.	SG.RA-3.1 Determine if the organization specifies the information and the Smart Grid information system impact levels. SG.RA-3.2 Determine if the organization documents the impact level results (including supporting rationale) in the security plan for information and the Smart Grid information system. SG.RA-3.3 Determine if the organization reviews the Smart Grid information system and information impact levels on an organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Risk assessment policy; procedures addressing security categorization of organizational information and Smart Grid information systems; security planning policy and procedures; security plan; security categorization documentation; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security categorization and risk assessment responsibilities].
SG.RA-4	Risk Assessment	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Conducts assessments of risk from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and Smart Grid information systems; and 2. Updates risk assessments on an organization-defined frequency or whenever significant changes occur to the Smart Grid information system or environment of operation, or other conditions that may impact the security of the Smart Grid information system. Supplemental Guidance Risk assessments take into account vulnerabilities, threat sources, risk tolerance levels, and security mechanisms planned or in place to determine the resulting level of residual risk posed to organizational operations, organizational assets, or individuals based on the operation of the Smart Grid information system. Requirement Enhancements None. Additional Considerations	SG.RA-4.1 Determine if the organization conducts assessments of risk from a) the unauthorized access of information and Smart Grid information systems b) use of information and Smart Grid information systems c) disclosure of information and Smart Grid information systems d) disruption of information and Smart Grid information systems e) modification of information and Smart Grid information systems f) destruction of information and Smart Grid information systems. SG.RA-4.2 Determine if the organization updates risk assessments on an organization-defined frequency or whenever significant changes occur to the Smart Grid information system or environment of operation, or other conditions that may impact the security of the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with risk assessment responsibilities].
SG.RA-5	Risk Assessment Update	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization updates the risk assessment plan on an organization-defined frequency or whenever significant changes occur to the Smart Grid information system, the facilities where the Smart Grid information system resides, or other conditions that may affect the security or authorization-to-operate status of the Smart Grid information system. Supplemental Guidance The organization develops and documents specific criteria for what are considered significant changes to the Smart Grid information system. Requirement Enhancements None. Additional Considerations None.	SG.RA-5.1 Determine if the organization updates the risk assessment plan on an organization-defined frequency or whenever significant changes occur to the Smart Grid information system, the facilities where the Smart Grid information system resides, or other conditions that may affect the security or authorization-to-operate status of the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: Risk assessment policy; security planning policy and procedures; procedures addressing organizational assessments of risk; security plan; risk assessment; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with risk assessment responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.RA-6	Vulnerability Assessment and Awareness	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Monitors and evaluates the Smart Grid information system according to the risk management plan on an organization-defined frequency to identify vulnerabilities that might affect the security of a Smart Grid information system; 2. Analyzes vulnerability scan reports and remediates vulnerabilities within an organization-defined time frame based on an assessment of risk; 3. Shares information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other Smart Grid information systems; 4. Updates the Smart Grid information system to address any identified vulnerabilities in accordance with organization's Smart Grid information system maintenance policy; and 5. Updates the list of Smart Grid information system vulnerabilities on an organization-defined frequency or when new vulnerabilities are identified and reported. Supplemental Guidance Vulnerability analysis for custom software and applications may require additional, more specialized approaches (e.g., vulnerability scanning tools to scan for Web-based vulnerabilities, source code reviews, and static analysis of source code). Vulnerability scanning includes scanning for ports, protocols, and services that should not be accessible to users and for improperly configured or incorrectly operating information flow mechanisms. Requirement Enhancements 1. The organization employs vulnerability scanning tools that include the capability to update the list of Smart Grid information system vulnerabilities scanned; and 2. The organization includes privileged access authorization to organization-defined Smart Grid information system components for selected vulnerability scanning activities to facilitate more thorough scanning. Additional Considerations A1. The organization employs automated mechanisms on an organization-defined frequency to detect the presence of unauthorized software on organizational Smart Grid information systems and notifies designated organizational officials; A2. The organization performs security testing to determine the level of difficulty in circumventing the security requirements of the Smart Grid information system; and A3. The organization employs automated mechanisms to compare the results of vulnerability scans over time to determine trends in Smart Grid information system vulnerabilities.	SG.RA-6.1 Determine if: (i) the organization monitors the Smart Grid information system according to the risk management plan on an organization-defined frequency to identify vulnerabilities that might affect the security of a Smart Grid information system; (ii) the organization evaluates the Smart Grid information system according to the risk management plan on an organization-defined frequency to identify vulnerabilities that might affect the security of a Smart Grid information system. SG.RA-6.2 Determine if: (i) the organization analyzes vulnerability scan reports within an organization-defined time frame based on an assessment of risk; (ii) the organization remediates vulnerabilities within an organization-defined time frame based on an assessment of risk. SG.RA-6.3 Determine if the organization shares information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other Smart Grid information systems. SG.RA-6.4 Determine if the organization updates the Smart Grid information system to address any identified vulnerabilities in accordance with organization's Smart Grid information system maintenance policy. SG.RA-6.5 Determine if the organization updates the list of Smart Grid information system vulnerabilities on an organization-defined frequency or when new vulnerabilities are identified and reported. SG.RA-6.6 (requirement enhancement 1) Determine if the organization employs vulnerability scanning tools that include the capability to update the list of Smart Grid information system vulnerabilities scanned. SG.RA-6.7 (requirement enhancement 2) Determine if the organization includes privileged access authorization to organization-defined Smart Grid information system components for selected vulnerability scanning activities to facilitate more thorough scanning.	Examine, Interview, Test	Examine: [SELECT FROM: Risk assessment policy; procedures addressing vulnerability scanning; security plan; Smart Grid information system design documentation; list of unauthorized software; notifications or alerts of unauthorized software on organizational Smart Grid information systems; list of Smart Grid information system components for vulnerability scanning; personnel access authorization list; authorization credentials; access authorization records; vulnerability scanning tools and techniques documentation; penetration test results; vulnerability scanning results; vulnerability scanning tools and techniques documentation; patch and vulnerability management records; records of updates to vulnerabilities scanned; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with risk assessment and vulnerability scanning responsibilities]. Test: [SELECT FROM: Vulnerability scanning capability and associated scanning tools].
			Smart Grid Information System and Services Acquisition (SG.SA)			
SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented Smart Grid information system and services acquisition security policy that addresses— i. The objectives, roles, and responsibilities for the Smart Grid information system and services acquisition security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the Smart Grid information system and services acquisition security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the Smart Grid information system and services acquisition policy and associated physical and environmental protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the Smart Grid information system and services acquisition policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The Smart Grid information system and services acquisition policy can be included as part of the general information security policy for the organization. Smart Grid information system and services acquisition procedures can be developed for the security program in general and for a particular Smart Grid information system when required. Requirement Enhancements None.	SG.SA-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency a) A documented Smart Grid information system and services acquisition security policy that addresses 1) The objectives, roles, and responsibilities for the risk assessment security program as it relates to protecting the organization's personnel and assets; and 2) The scope of the risk assessment security program as it applies to all of the organizational staff, contractors, and third parties; and b) Procedures to address the implementation of the risk assessment security policy and associated risk assessment protection requirements. SG.SA-1.2 Determine if: (i) the organization documents management commitment ensures compliance with the organization's security policy and other regulatory requirements; (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG.SA-1.3 Determine if the organization ensures that the Smart Grid information system and services acquisition security policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SA-2	Security Policies for Contractors and Third Parties	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. External suppliers and contractors that have an impact on the security of Smart Grid information systems must meet the organization's policy and procedures; and 2. The organization establishes procedures to remove external supplier and contractor access to Smart Grid information systems at the conclusion/termination of the contract. Supplemental Guidance The organization considers the increased security risk associated with outsourcing as part of the decision-making process to determine what to outsource and what outsourcing partner to select. Contracts with external suppliers govern physical as well as logical access. The organization considers confidentiality or nondisclosure agreements and intellectual property rights. Requirement Enhancements None. Additional Considerations None.	SG.SA-2.1 Determine if the organization's external suppliers and contractors that have an impact on the security of Smart Grid information systems must meet the organization's policy and procedures. SG.SA-2.2 Determine if: (i) the organization establishes procedures to remove external supplier and contractor access to Smart Grid information systems at the conclusion/termination of the contract; (ii) the organization documents procedures to remove external supplier and contractor access to Smart Grid information systems at the conclusion/termination of the contract.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy and procedures; Personnel security policy; procedures addressing personnel sanctions; third party policy; third party standards and procedures; rules of behavior; records of formal sanctions; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with personnel security responsibilities; Organizational personnel with third party security responsibilities; Organizational personnel with system and services acquisition responsibilities].
SG.SA-3	Life-Cycle Support	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization manages the Smart Grid information system using a system development lifecycle methodology that includes security. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations	SG.SA-3.1 Determine if the organization manages the Smart Grid information system using a system development lifecycle methodology that includes security.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing the integration of information security into the system development life cycle process; Smart Grid information system development life cycle documentation; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with information security and system life cycle development responsibilities].
SG.SA-4	Acquisitions	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization includes security requirements in Smart Grid information system acquisition contracts in accordance with applicable laws, regulations, and organization-defined security policies. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations	SG.SA-4.1 Determine if the organization includes security requirements in Smart Grid information system acquisition contracts in accordance with applicable laws, regulations, and organization-defined security policies.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing the integration of information security requirements and / or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for Smart Grid information systems or services; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities].
SG.SA-5	Smart Grid Information System Documentation	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirement Requirement 1. Smart Grid information system documentation includes how to configure, install, and use the information system and the information system's security features; and 2. The organization obtains from the contractor/third-party, information describing the functional properties of the security controls employed within the Smart Grid information system. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations	SG.SA-5.1 Determine if the Smart Grid information system documentation includes a) how to configure the Smart Grid information system and the Smart Grid information system's security features; b) install the Smart Grid information system and the Smart Grid information system's security features; c) use the Smart Grid information system and the Smart Grid information system's security features. SG.SA-5.2 Determine if the organization obtains from the contractor/third-party, information describing the functional properties of the security controls employed within the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing Smart Grid information system documentation; Smart Grid information system design documentation; Smart Grid information system documentation including administrator and user guides; records documenting attempts to obtain unavailable or nonexistent Smart Grid information system documentation; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system documentation responsibilities; organizational personnel operating, using, and / or maintaining the Smart Grid information system; Organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities; organizational personnel operating, using, and / or maintaining the Smart Grid information system].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SA-6	Software License Usage Restrictions	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Uses software and associated documentation in accordance with contract agreements and copyright laws; and 2. Controls the use of software and associated documentation protected by quantity licenses and copyrighted material. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations None.	SG.SA-6.1 Determine if the organization uses software and associated documentation in accordance with contract agreements and copyright laws. SG.SA-6.2 Determine if the organization controls the use of software and associated documentation protected by quantity licenses and copyrighted material.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing software usage restrictions; site license documentation; list of software usage restrictions; procedures addressing the integration of information security requirements and / or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for Smart Grid information systems or services; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system administration responsibilities; organizational personnel operating, using, and / or maintaining the Smart Grid information system].
SG.SA-7	User-Installed Software	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization establishes policies and procedures to manage user installation of software. Supplemental Guidance If provided the necessary privileges, users have the ability to install software. The organization's security program identifies the types of software permitted to be downloaded and installed (e.g., updates and security patches to existing software) and types of software prohibited (e.g., software that is free only for personal, not corporate use, and software whose pedigree with regard to being potentially malicious is unknown or suspect). Requirement Enhancements None. Additional Considerations	SG.SA-7.1 Determine if the organization establishes policies and procedures to manage user installation of software.	Examine, Interview, Test	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing user installed software; list of rules governing user installed software; network traffic on the Smart Grid information system; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system administration responsibilities; organizational personnel operating, using, and / or maintaining the Smart Grid information system]. Test: [SELECT FROM: Enforcement of rules for user installed software on the Smart Grid information system; Smart Grid information system for prohibited software].
SG.SA-8	Security Engineering Principles	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization applies security engineering principles in the specification, design, development, and implementation of any Smart Grid information system. Security engineering principles include: 1. Ongoing secure development education requirements for all developers involved in the Smart Grid information system; 2. Specification of a minimum standard for security; 3. Specification of a minimum standard for privacy; 4. Creation of a threat model for a Smart Grid information system; 5. Updating of product specifications to include mitigations for threats discovered during threat modeling; 6. Use of secure coding practices to reduce common security errors; 7. Testing to validate the effectiveness of secure coding practices; 8. Performance of a final security audit prior to authorization to operate to confirm adherence to security requirements; 9. Creation of a documented and tested security response plan in the event vulnerability is discovered; 10. Creation of a documented and tested privacy response plan in the event vulnerability is discovered; and 11. Performance of a root cause analysis to understand the cause of identified vulnerabilities. Supplemental Guidance The application of security engineering principles is primarily targeted at new development Smart Grid information systems or Smart Grid information systems undergoing major upgrades. These principles are integrated into the Smart Grid information system development life cycle. For legacy Smart Grid information systems, the organization applies security engineering principles to Smart Grid information system upgrades and modifications, to the extent feasible, given the current state of the hardware, software, and firmware components within the Smart Grid information system. The organization minimizes risk to legacy systems through attack surface reduction and other mitigating controls. Requirement Enhancements None. Additional Considerations None.	SG.SA-8.1 Determine if: (i) the organization applies security engineering principles in the a) specification of any Smart Grid information system; b) design of any Smart Grid information system; c) development of any Smart Grid information system; d) implementation of any Smart Grid information system. (ii) the organization's security engineering principles include: a) Ongoing secure development education requirements for all developers involved in the Smart Grid information system; b) Specification of a minimum standard for security; c) Specification of a minimum standard for privacy; d) Creation of a threat model for a Smart Grid information system; e) Updating of product specifications to include mitigations for threats discovered during threat modeling; f) Use of secure coding practices to reduce common security errors; g) Testing to validate the effectiveness of secure coding practices; h) Performance of a final security audit prior to authorization to operate to confirm adherence to security requirements; i) Creation of a documented and tested security response plan in the event vulnerability is discovered; j) Creation of a documented and tested privacy response plan in the event vulnerability is discovered; k) Performance of a root cause analysis to understand the cause of identified vulnerabilities.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing security engineering principles used in the development and implementation of the Smart Grid information system; Smart Grid information system design documentation; security requirements and security specifications for the Smart Grid information system; penetration test and vulnerability scan reports; security test and evaluation results; authority to operate documentation; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system design, development, implementation, and modification responsibilities; Organizational personnel with system and services acquisition responsibilities; Smart Grid information system authorizing official].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SA-9	Developer Configuration Management	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization requires that Smart Grid information system developers/integrators document and implement a configuration management process that— 1. Manages and controls changes to the Smart Grid information system during design, development, implementation, and operation; 2. Tracks security flaws; and 3. Includes organizational approval of changes. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization requires that Smart Grid information system developers/integrators provide an integrity check of delivered software and firmware.	SG.SA-9.1 Determine if the organization requires that Smart Grid information system developers/integrators document and implement a configuration management process that a) Manages changes to the Smart Grid information system during design, development, implementation, and operation; b) Controls changes to the Smart Grid information system during design, development, implementation, and operation; c) Tracks security flaws; d) Tracks security flaws; e) Includes organizational approval of changes.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing Smart Grid information system developer / integrator configuration management; acquisition contracts and service level agreements; Smart Grid information system developer / integrator configuration management plan; security flaw tracking records; system change authorization records; Smart Grid information system configuration management plan; other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with Smart Grid information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities].
SG.SA-10	Developer Security Testing	Tech	Category: Common Technical Requirements, Integrity Requirement 1. The Smart Grid information system developer creates a security test and evaluation plan; 2. The developer submits the plan to the organization for approval and implements the plan once written approval is obtained; 3. The developer documents the results of the testing and evaluation and submits them to the organization for approval; and 4. The organization does not perform developmental security tests on the production Smart Grid information system. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization requires that Smart Grid information system developers employ code analysis tools to examine software for common flaws and document the results of the analysis; and A2. The organization requires that Smart Grid information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.	SG.SA-10.1 Determine if the Smart Grid information system developer creates a security test and evaluation plan. SG.SA-10.2 Determine if the developer submits the plan to the organization for approval and implements the plan once written approval is obtained. SG.SA-10.3 Determine if the developer documents the results of the testing and evaluation and submits them to the organization for approval. SG.SA-10.4 Determine if: (i) the organization prohibits developmental security tests on the production Smart Grid information system; (ii) the organization enforces prohibiting developmental security tests on the production Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing Smart Grid information system developer / integrator security testing; acquisition contracts and service level agreements; Smart Grid information system developer / integrator security test plans; records of developer / integrator security testing results for the Smart Grid information system; security flaw tracking records; vulnerability scanning results; Smart Grid information system risk assessment reports; acquisition documentation; acquisition contracts for Smart Grid information systems or services; security test and evaluation plan; security test and evaluation results report; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with developer security testing responsibilities].
SG.SA-11	Supply Chain Protection	Tech	Category: Common Technical Requirements, Integrity Requirement The organization protects against supply chain vulnerabilities employing requirements defined to protect the products and services from threats initiated against organizations, people, information, and resources, possibly international in scope, that provides products or services to the organization. Supplemental Guidance Supply chain protection helps to protect Smart Grid information systems (including the technology products that compose those Smart Grid information systems) throughout the system development life cycle (e.g., during design and development, manufacturing, packaging, assembly, distribution, system integration, operations, maintenance, and retirement). Requirement Enhancements None. Additional Considerations A1. The organization conducts a due diligence review of suppliers prior to entering into contractual agreements to acquire Smart Grid information system hardware, software, firmware, or services; A2. The organization uses a diverse set of suppliers for Smart Grid information systems, Smart Grid information system components, technology products, and Smart Grid information system services; and A3. The organization employs independent analysis and penetration testing against delivered Smart Grid information systems, Smart Grid information system components, and technology products.	SG.SA-11.1 Determine if the organization protects against supply chain vulnerabilities employing requirements defined to protect the products and services from threats initiated against a) organizations, that provides products or services to the organization; b) people, that provides products or services to the organization; c) information, that provides products or services to the organization; d) resources, that provides products or services to the organization.	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing supply chain protection; procedures addressing the integration of information security requirements and / or security specifications into the acquisition process; solicitation documents; acquisition documentation; acquisition contracts for Smart Grid information systems or services; acquisition contracts and service level agreements; list of supply chain threats; list of measures to be taken against supply chain threats; Smart Grid information system development life cycle documentation; due diligence reviews documentation; procedures addressing the baseline configuration of the Smart Grid information system; configuration management plan; Smart Grid information system design documentation; Smart Grid information system architecture and configuration documentation; penetration testing records; security test and evaluation results reports; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with supply chain protection responsibilities; organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities].
Smart Grid Information System and Communication Protection (SG.SC)						

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SC-1	System and Communication Protection Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented Smart Grid information system and communication protection security policy that addresses— i. The objectives, roles, and responsibilities for the Smart Grid information system and communication protection security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the Smart Grid information system and communication protection policy as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the Smart Grid information system and communication protection security policy and associated Smart Grid information system and communication protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the Smart Grid information system and communication protection policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The Smart Grid information system and communication protection policy may be included as part of the general information security policy for the organization. Smart Grid information system and communication protection procedures can be developed for the security program in general and a Smart Grid information system in particular, when required. Requirement Enhancements None. Additional Considerations None.	SG.SC-1.1 Determine if the organization develops, implements, reviews, and updates on an organization-defined frequency a) A documented Smart Grid information system and communication protection security policy that addresses— 1) The objectives, roles, and responsibilities for the Smart Grid information system and communication protection security program as it relates to protecting the organization's personnel and assets; and 2) The scope of the Smart Grid information system and communication protection policy as it applies to all of the organizational staff, contractors, and third parties; and b) Procedures to address the implementation of the Smart Grid information system and communication protection security policy and associated Smart Grid information system and communication protection requirements. SG.SC-1.2 Determine if: (i) the organization documents management commitment ensures compliance with the organization's security policy and other regulatory requirements; (ii) management commitment ensures compliance with the organization's security policy and other regulatory requirements. SG.AC-1.3 Determine if the organization ensures that the Smart Grid information system and communication protection policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.SC-2	Communications Partitioning	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system partitions the communications for telemetry/data acquisition services and management functionality. Supplemental Guidance The Smart Grid information system management communications path needs to be physically or logically separated from the telemetry/data acquisition services communications path. Requirement Enhancements None. Additional Considerations --	SG.SC-2.1 Determine if the Smart Grid information system partitions the communications for telemetry/data acquisition services and management functionality.	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; procedures addressing communication partitioning; procedures addressing quality of services; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel installing, configuring, and / or maintaining communications].
SG.SC-3	Security Function Isolation	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system isolates security functions from nonsecurity functions. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system employs underlying hardware separation mechanisms to facilitate security function isolation; and A2. The Smart Grid information system isolates security functions (e.g., functions enforcing access and information flow control) from both nonsecurity functions and from other security functions.	SG.SC-3.1 Determine if the Smart Grid information system isolates security functions from nonsecurity functions.	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; procedures addressing security function isolation; list of critical security functions; list of security functions to be isolated from nonsecurity functions; Smart Grid information system design documentation; hardware separation mechanisms; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Test: [SELECT FROM: Separation of security functions from nonsecurity functions within the Smart Grid information system; Hardware separation mechanisms facilitating security function isolation; Isolation of security functions enforcing access and information flow control].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SC-4	Information Remnants	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system prevents unauthorized or unintended information transfer via shared Smart Grid information system resources. Supplemental Guidance Control of Smart Grid information system remnants, sometimes referred to as object reuse, or data remnants, prevents information from being available to any current user/role/process that obtains access to a shared Smart Grid information system resource after that resource has been released back to the Smart Grid information system. Requirement Enhancements None. Additional Considerations	SG.SC-4.1 Determine if the Smart Grid information system prevents unauthorized or unintended information transfer via shared Smart Grid information system resources.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing information remnants; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Test: [SELECT FROM: Smart Grid information system for unauthorized and unintended transfer of information via shared system resources].
SG.SC-5	Denial-of-Service Protection	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system mitigates or limits the effects of denial-of-service attacks based on an organization-defined list of denial-of-service attacks. Supplemental Guidance Network perimeter devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial-of-service attacks. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system restricts the ability of users to launch denial-of-service attacks against other Smart Grid information systems or networks; and A2. The Smart Grid information system manages excess capacity, bandwidth, or other redundancy to limit the effects of information flooding types of denial-of-service attacks.	SG.SC-5.1 Determine if: (i) the Smart Grid information system mitigates or limits the effects of denial-of-service attacks based on an organization-defined list of denial-of-service attacks; (ii) the organization documents a defined list of denial-of-service attacks against the Smart Grid information systems.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing denial of service protection; Smart Grid information system design documentation; security plan; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Test: [SELECT FROM: Smart Grid information system for protection against or limitation of the effects of denial of service attacks; Automated mechanisms implementing Smart Grid information system bandwidth, capacity, and redundancy management].
SG.SC-6	Resource Priority	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system prioritizes the use of resources. Supplemental Guidance Priority protection helps prevent a lower-priority process from delaying or interfering with the Smart Grid information system servicing any higher-priority process. This requirement does not apply to components in the Smart Grid information system for which only a single user/role exists. Requirement Enhancements None. Additional Considerations	SG.SC-6.1 Determine if the Smart Grid information system prioritizes the use of resources.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing prioritization of Smart Grid information system resources; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing resource allocation capability].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SC-7	Boundary Protection	Tech	Category: Unique Technical Requirements Requirement 1. The organization defines the boundary of the Smart Grid information system; 2. The Smart Grid information system monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; 3. The Smart Grid information system connects to external networks or information systems only through managed interfaces consisting of boundary protection devices; 4. The managed interface implements security measures appropriate for the protection of integrity and confidentiality of the transmitted information; and 5. The organization prevents public access into the organization's internal Smart Grid information system networks except as appropriately mediated. Supplemental Guidance Managed interfaces employing boundary protection devices include proxies, gateways, routers, firewalls, guards, or encrypted tunnels. Requirement Enhancements 1. The Smart Grid information system denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception); 2. The Smart Grid information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination; and 3. Communications to/from Smart Grid information system components shall be restricted to specific components in the Smart Grid information system. Communications shall not be permitted to/from any non-Smart Grid system unless separated by a controlled logical/physical interface. Additional Considerations A1. The organization prevents the unauthorized release of information outside the Smart Grid information system boundary or any unauthorized communication through the Smart Grid information system boundary when an operational failure occurs of the boundary protection mechanisms; A2. The organization prevents the unauthorized exfiltration of information across managed interfaces; A3. The Smart Grid information system routes internal communications traffic to the Internet through authenticated proxy servers within the managed interfaces of boundary protection devices; A4. The organization limits the number of access points to the Smart Grid information system to allow for better monitoring of inbound and outbound network traffic; A5. Smart Grid information system boundary protections at any designated alternate processing/control sites provide the same levels of protection as that of the primary site; and A6. The Smart Grid information system fails securely in the event of an operational failure of a boundary protection device.	SG.SC-7.1 Determine if the organization defines the boundary of the Smart Grid information system. SG.SC-7.2 Determine if: (i) the Smart Grid information system monitors communications at the external boundary of the system and at key internal boundaries within the system; (ii) the Smart Grid information system controls communications at the external boundary of the system and at key internal boundaries within the system. SG.SC-7.3 Determine if the Smart Grid information system connects to external networks or Smart Grid information systems only through managed interfaces consisting of boundary protection devices. SG.SC-7.4 Determine if the managed interface implements security measures appropriate for the protection of integrity and confidentiality of the transmitted information. SG.SC-7.5 Determine if the organization prevents public access into the organization's internal Smart Grid information system networks except as appropriately mediated. SG.SC-7.6 (requirement enhancement 1) Determine if: (i) the Smart Grid information system denies network traffic by default; (ii) the Smart Grid information system allows network traffic by exception. SG.SC-7.7 (requirement enhancement 2) Determine if the Smart Grid information system checks incoming communications to ensure that the communications are coming from an authorized source and routed to an authorized destination. SG.SC-7.8 (requirement enhancement 3) Determine if: (i) communications to/from Smart Grid information system components shall be restricted to specific components in the Smart Grid information system; (ii) communications shall restricted to/from any non-Smart Grid information system unless separated by a controlled logical/physical interface.	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing boundary protection; list of key internal boundaries of the Smart Grid information system; list of mediation vehicles for allowing public access to the organization's internal networks; Smart Grid information system design documentation; boundary protection hardware and software; traffic flow policy; Smart Grid information system security architecture; boundary protection hardware and software; records of traffic flow policy exceptions; Smart Grid information system hardware and software; Smart Grid information system architecture; Smart Grid information system configuration settings and associated documentation; facility communications and wiring diagram; Smart Grid information system architecture; Smart Grid information system audit records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific boundary ownership and responsibilities]. Test: [SELECT FROM: Automated mechanisms implementing boundary protection capability within the Smart Grid information system; Automated mechanisms implementing access controls for public access to the organization's internal networks; Managed interfaces implementing organizational traffic flow policy; Automated mechanisms supporting the fail-safe boundary protection capability within the Smart Grid information system; Automated mechanisms supporting non-remote connections with the Smart Grid information system; Mechanisms implementing managed interfaces within Smart Grid information system boundary protection devices; Automated mechanisms preventing unauthorized exfiltration of information across managed interfaces; Automated mechanisms implementing host-based boundary protection capability; Physical access capability implementing protections against unauthorized physical connections to the Smart Grid information system; Mechanisms routing networked, privileged access through dedicated managed interfaces; Mechanisms preventing discovery of system components at a managed interface].
SG.SC-8	Communication Integrity	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system protects the integrity of electronically communicated information. Supplemental Guidance None. Requirement Enhancements 1. The organization employs cryptographic mechanisms to ensure integrity. Additional Considerations A1. The Smart Grid information system maintains the integrity of information during aggregation, packaging, and transformation in preparation for transmission.	SG.SC-8.1 Determine if the Smart Grid information system protects the integrity of electronically communicated information. SG.SC-8.2 (requirement enhancement 1) Determine if the organization employs cryptographic mechanisms to ensure integrity of Smart Grid information system information.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing transmission integrity; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Test: [SELECT FROM: Transmission integrity capability within the Smart Grid information system; Cryptographic mechanisms implementing transmission integrity capability within the Smart Grid information system; Transmission integrity capability within the Smart Grid information system].
SG.SC-9	Communication Confidentiality	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system protects the confidentiality of communicated information. Supplemental Guidance None. Requirement Enhancements 1. The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission. Additional Considerations None.	SG.SC-9.1 Determine if the Smart Grid information system protects the confidentiality of communicated information. SG.SC-9.2 (requirement enhancement 1) Determine if the organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission of Smart Grid information system information.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing transmission confidentiality; Smart Grid information system design documentation; Smart Grid information system communications hardware and software or Protected Distribution System protection mechanisms; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Test: [SELECT FROM: Cryptographic mechanisms implementing transmission confidentiality capability within the Smart Grid information system; Transmission confidentiality capability within the Smart Grid information system; Transmission confidentiality capability within the Smart Grid information system].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SC-10	Trusted Path	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system establishes a trusted communications path between the user and the Smart Grid information system. Supplemental Guidance A trusted path is the means by which a user and target of evaluation security functionality can communicate with the necessary confidence. Requirement Enhancements None. Additional Considerations --	SG.SC-10.1 Determine if: (i) the Smart Grid information system establishes a trusted communications path between the user and the Smart Grid information system. (ii) the Smart Grid information system documents trusted communications path between the user and the Smart Grid information system.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing trusted communications paths; security plan; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing trusted communications paths within the Smart Grid information system].
SG.SC-11	Cryptographic Key Establishment and Management	Tech	Category: Common Technical Requirements, Confidentiality Requirement The organization establishes and manages cryptographic keys for required cryptography employed within the information system. Supplemental Guidance Key establishment includes a key generation process in accordance with a specified algorithm and key sizes, and key sizes based on an assigned standard. Key generation must be performed using an appropriate random number generator. The policies for key management need to address such items as periodic key changes, key destruction, and key distribution. Requirement Enhancements 1. The organization maintains availability of information in the event of the loss of cryptographic keys by users. See Chapter 4 for key management requirements. Additional Considerations None.	SG.SC-11.1 Determine if: (i) the organization establishes cryptographic keys for required cryptography employed within the Smart Grid information system; (ii) the organization manages cryptographic keys for required cryptography employed within the Smart Grid information system. SG.SC-11.2 (requirement enhancement 1) Determine if: (i) the key establishment includes a key generation process in accordance with a specified algorithm and key sizes, and key sizes based on an assigned standard; (ii) the key generation must be performed using an appropriate random number generator; (iii) the policies for key management need to address such items as periodic key changes, key destruction, and key distribution.	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing cryptographic key management and establishment; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for cryptographic key establishment or management]. Test: [SELECT FROM: Automated mechanisms implementing cryptographic key management and establishment within the Smart Grid information system].
SG.SC-12	Use of Validated Cryptography	Tech	Category: Common Technical Requirements, Confidentiality Requirement All of the cryptography and other security functions (e.g., hashes, random number generators, etc.) that are required for use in a Smart Grid information system shall be NIST Federal Information Processing Standard (FIPS) approved or allowed for use in FIPS modes. Supplemental Guidance For a list of current FIPS-approved or allowed cryptography, see Chapter Four Cryptography and Key Management. Requirement Enhancements None. Additional Considerations	SG.SC-12.1 Determine if: (i) the organization documents all of the cryptography and other cryptographic security functions (e.g., hashes, random number generators, etc.) that are required for use in a Smart Grid information system; (ii) all cryptography and other cryptographic security functions shall be NIST Federal Information Processing Standard (FIPS) approved or allowed for use in FIPS modes.	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing use of cryptography; FIPS cryptography standards; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; cryptographic module validation certificates; cryptographic module validation certificates; NIST cryptographic standards; FIPS cryptographic module validation certificates; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for implementing cryptography within the Smart Grid information system]. Test: [SELECT FROM: Automated mechanisms implementing cryptographic key management and establishment within the Smart Grid information system].
SG.SC-13	Collaborative Computing	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization develops, disseminates, and periodically reviews and updates on an organization-defined frequency a collaborative computing policy. Supplemental Guidance Collaborative computing mechanisms include video and audio conferencing capabilities or instant messaging technologies. Explicit indication of use includes signals to local users when cameras and/or microphones are activated. Requirement Enhancements None. Additional Considerations None.	SG.SC-13.1 Determine if: (i) the organization develops an organization-defined frequency a collaborative computing policy; (ii) the organization disseminates an organization-defined frequency a collaborative computing policy; (iii) the organization periodically reviews on an organization-defined frequency a collaborative computing policy; (iv) the organization periodically updates on an organization-defined frequency a collaborative computing policy.	Examine	Examine: [SELECT FROM: System and communications protection policy; procedures addressing collaborative computing; access control policy and procedures; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SC-14	Transmission of Security Parameters	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system reliably associates security parameters with information exchanged between the enterprise information systems and the Smart Grid information system. Supplemental Guidance Security parameters may be explicitly or implicitly associated with the information contained within the Smart Grid information system. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system validates the integrity of security parameters exchanged between Smart Grid information systems.	SG.SC-14.1 Determine if the Smart Grid information system reliably associates security parameters with information exchanged between the enterprise Smart Grid information systems and the Smart Grid information system.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing transmission of security parameters; access control policy and procedures; boundary protection procedures; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms supporting reliable transmission of security parameters between Smart Grid information systems].
SG.SC-15	Public Key Infrastructure Certificates	Tech	Category: Common Technical Requirements, Confidentiality Requirement For Smart Grid information systems that implement a public key infrastructure, the organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider. Supplemental Guidance Registration to receive a public key certificate needs to include authorization by a supervisor or a responsible official and needs to be accomplished using a secure process that verifies the identity of the certificate holder and ensures that the certificate is issued to the intended party. Requirement Enhancements None. Additional Considerations	SG.SC-15.1 Determine if for Smart Grid information systems that implement a public key infrastructure, the organization issues public key certificates under an appropriate certificate policy or obtains public key certificates under an appropriate certificate policy from an approved service provider.	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing public key infrastructure certificates; public key certificate policy or policies; public key issuing process; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with public key infrastructure certificate issuing responsibilities]. Test: [SELECT FROM: Automated mechanisms supporting reliable transmission of security parameters between Smart Grid information systems through the use of public key infrastructures].
SG.SC-16	Mobile Code	Tech	Category: Common Technical Requirements, Confidentiality Requirement The organization— 1. Establishes usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the Smart Grid information system if used maliciously; 2. Documents, monitors, and manages the use of mobile code within the Smart Grid information system; and 3. A management authority authorizes the use of mobile code. Supplemental Guidance Mobile code technologies include, for example, Java, JavaScript, ActiveX, PDF, Postscript, Shockwave movies, Flash animations, and VBScript. Usage restrictions and implementation guidance need to apply to both the selection and use of mobile code installed on organizational servers and mobile code downloaded and executed on individual workstations. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system implements detection and inspection mechanisms to identify unauthorized mobile code and takes corrective actions, when necessary.	SG.SC-16.1 Determine if: (i) the organization establishes usage restrictions for mobile code technologies based on the potential to cause damage to the Smart Grid information system if used maliciously; (ii) the organization establishes implementation guidance for mobile code technologies based on the potential to cause damage to the Smart Grid information system if used maliciously. SG.SC-16.2 Determine if the organization a) documents the use of mobile code within the Smart Grid information system; b) monitors the use of mobile code within the Smart Grid information system; c) manages the use of mobile code within the Smart Grid information system. SG.SC-16.3 Determine if: (i) the organization documents a management authority to authorize the use of mobile code; (ii) a management authority authorizes the use of mobile code.	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions; mobile code usage restrictions, mobile code implementation policy and procedures; list of acceptable mobile code and mobile code technologies; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system audit records; acquisition documentation; acquisition contracts for Smart Grid information systems or services; list of applications for which automatic execution of mobile code must be prohibited; list of actions required before execution of mobile code; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with mobile code authorization, monitoring, and control responsibilities; Organizational personnel with mobile code management responsibilities; organizational personnel with Smart Grid information system security, acquisition, and contracting responsibilities]. Test: [SELECT FROM: Mobile code authorization and monitoring capability for the organization; Automated mechanisms implementing mobile code detection and inspection capability; Automated mechanisms preventing download and execution of prohibited mobile code; Automated mechanisms preventing mobile code execution within the Smart Grid information system].
SG.SC-17	Voice-Over Internet Protocol	Tech	Category: Unique Technical Requirements Requirement The organization— 1. Establishes usage restrictions and implementation guidance for VoIP technologies based on the potential to cause damage to the Smart Grid information system if used maliciously; and 2. Authorizes, monitors, and controls the use of VoIP within the Smart Grid information system. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations	SG.SC-17.1 Determine if: (i) the organization establishes usage restrictions for VoIP technologies based on the potential to cause damage to the Smart Grid information system if used maliciously; (ii) the organization establishes implementation guidance for VoIP technologies based on the potential to cause damage to the Smart Grid information system if used maliciously. SG.SC-17.2 Determine if the organization a) authorizes the use of VoIP within the Smart Grid information system; b) monitors the use of VoIP within the Smart Grid information system; c) controls the use of VoIP within the Smart Grid information system.	Examine, Interview, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing VoIP; VoIP usage restrictions; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with VoIP authorization and monitoring responsibilities]. Test: [SELECT FROM: VoIP authorization and monitoring capability for the organization].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SC-18	System Connections	Tech	Category: Common Technical Requirements, Confidentiality Requirement All external Smart Grid information system and communication connections are identified and protected from tampering or damage. Supplemental Guidance External access point connections to the Smart Grid information system need to be secured to protect the Smart Grid information system. Access points include any externally connected communication end point (for example, dial-up modems). Requirement Enhancements None. Additional Considerations None.	SG.SC-18.1 Determine if: (i) the organization documents all external Smart Grid information system and communication connections; (ii) the organization protects all external Smart Grid information system and communication connections from tampering or damage.	Examine, Interview	Examine: [SELECT FROM: Access control policy; procedures addressing Smart Grid information system connections; system and communications protection policy; Smart Grid information system interconnection security agreements; security plan; Smart Grid information system design documentation; security assessment report; plan of action and milestones; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibility for developing, implementing, or approving Smart Grid information system interconnection agreements].
SG.SC-19	Security Roles	Tech	Category: Common Technical Requirements, Integrity Requirement The Smart Grid information system design and implementation specifies the security roles and responsibilities for the users of the Smart Grid information system. Supplemental Guidance Security roles and responsibilities for Smart Grid information system users need to be specified, defined, and implemented based on the sensitivity of the information handled by the user. These roles may be defined for specific job descriptions or for individuals. Requirement Enhancements None. Additional Considerations	SG.SC-19.1 Determine if: (i) the Smart Grid information system design specifies the security roles and responsibilities for the users of the Smart Grid information system; (ii) the Smart Grid information system implementation specifies the security roles and responsibilities for the users of the Smart Grid information system	Examine, Interview	Examine: [SELECT FROM: System and services acquisition policy; procedures addressing Smart Grid information system developer / integrator configuration management; acquisition contracts and service level agreements; Smart Grid information system developer / integrator configuration management plan; security flaw tracking records; system change authorization records; Smart Grid information system configuration management plan; other relevant documents or records]. Interview: [SELECT FROM: Organization personnel with Smart Grid information system security, acquisition, and contracting responsibilities; organization personnel with configuration management responsibilities].
SG.SC-20	Message Authenticity	Tech	Category: Common Technical Requirements, Integrity Requirement The Smart Grid information system provides mechanisms to protect the authenticity of device-to-device communications. Supplemental Guidance Message authentication provides protection from malformed traffic, misconfigured devices, and malicious entities. Requirement Enhancements None. Additional Considerations A1. Message authentication mechanisms should be implemented at the protocol level for both serial and routable protocols.	SG.SC-20.1 Determine if the Smart Grid information system provides mechanisms to protect the authenticity of device-to-device communications.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing transmission integrity; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Test: [SELECT FROM: Transmission integrity capability within the Smart Grid information system; Cryptographic mechanisms implementing transmission integrity capability within the Smart Grid information system; Transmission integrity capability within the Smart Grid information system].
SG.SC-21	Secure Name/Address Resolution Service	Tech	Category: Common Technical Requirements, Integrity Requirement The organization is responsible for— 1. Configuring systems that provide name/address resolution to supply additional data origin and integrity artifacts along with the authoritative data returned in response to resolution queries; and 2. Configuring systems that provide name/address resolution to Smart Grid information systems, when operating as part of a distributed, hierarchical namespace, to provide the means to indicate the security status of child subspaces and, if the child supports secure resolution services, enabled verification of a chain of trust among parent and child domains. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations None.	SG.SC-21.1 Determine if the organization is responsible for a) Configuring systems that provide name/address resolution to supply additional data origin and integrity artifacts along with the authoritative data returned in response to resolution queries; b) Configuring systems that provide name/address resolution to Smart Grid information systems, when operating as part of a distributed, hierarchical namespace, to provide the means to indicate the security status of child subspaces and, if the child supports secure resolution services, enabled verification of a chain of trust among parent and child domains.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing secure name/address resolution service (authoritative source); Automated mechanisms implementing child subspace security status indicators and chain of trust verification for resolution services].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SC-22	Fail in Known State	Tech	Category: Common Technical Requirements, Integrity Requirement The Smart Grid information system fails to a known state for defined failures. Supplemental Guidance Failure in a known state can be interpreted by organizations in the context of safety or security in accordance with the organization's mission/business/operational needs. Failure in a known secure state helps prevent a loss of confidentiality, integrity, or availability in the event of a failure of the Smart Grid information system or a component of the Smart Grid information system. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system preserves defined system state information in failure.	SG.SC-22.1 Determine if: (i) the Smart Grid information system fails to a known state for defined failures; (ii) the organization documents what fails to a known state for defined failures consists of.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing Smart Grid information system failure; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; list of failures requiring Smart Grid information system to fail in a known state; state information to be preserved in system failure; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing fail-in-known-state capability].
SG.SC-23	Thin Nodes	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system employs processing components that have minimal functionality and data storage. Supplemental Guidance The deployment of Smart Grid information system components with minimal functionality (e.g., diskless nodes and thin client technologies) reduces the number of endpoints to be secured and may reduce the exposure of information, Smart Grid information systems, and services to a successful attack. Requirement Enhancements None. Additional Considerations None.	SG.SC-23.1 Determine if the Smart Grid information system employs processing components that have minimal functionality and data storage.	Examine	Examine: [SELECT FROM: System and communications protection policy; procedures addressing use of thin nodes; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]
SG.SC-24	Honeypots	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system includes components specifically designed to be the target of malicious attacks for the purpose of detecting, deflecting, analyzing, and tracking such attacks. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system includes components that proactively seek to identify Web-based malicious code.	SG.SC-24.1 Determine if the Smart Grid information system includes components specifically designed to be the target of malicious attacks for the purpose of a) detecting b) deflecting c) analyzing d) tracking attacks.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing use of honeypots; access control policy and procedures; boundary protection procedures; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms proactively seeking Web-based malicious code].
SG.SC-25	Operating System-Independent Applications	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system includes organization-defined applications that are independent of the operating system. Supplemental Guidance Operating system-independent applications are applications that can run on multiple operating systems. Such applications promote portability and reconstitution on different platform architectures, thus increasing the availability for critical functionality while an organization is under an attack exploiting vulnerabilities in a given operating system. Requirement Enhancements None. Additional Considerations None.	SG.SC-25.1 Determine if the Smart Grid information system includes organization-defined applications that are independent of the operating system.	Examine	Examine: [SELECT FROM: System and communications protection policy; procedures addressing operating system-independent applications; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; list of operating system-independent applications; other relevant documents or records]

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SC-26	Confidentiality of Information at Rest	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system employs cryptographic mechanisms for all critical security parameters (e.g., cryptographic keys, passwords, security configurations) to prevent unauthorized disclosure of information at rest. Supplemental Guidance For a list of current FIPS-approved or allowed cryptography, see Chapter Four Cryptography and Key Management. Requirement Enhancements None. Additional Considerations --	SG.SC-26.1 Determine if the Smart Grid information system employs cryptographic mechanisms for all critical security parameters (e.g., cryptographic keys, passwords, security configurations) to prevent unauthorized disclosure of information at rest.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing protection of information at rest; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; cryptographic mechanisms and associated configuration documentation; list of information at rest requiring confidentiality and integrity protections; other relevant documents or records]. Test: [SELECT FROM: Automated mechanisms implementing confidentiality and integrity protections for information at-rest; Cryptographic mechanisms implementing confidentiality and integrity protections for information at-rest].
SG.SC-27	Heterogeneity	Tech	Category: Unique Technical Requirements Requirement The organization employs diverse technologies in the implementation of the Smart Grid information system. Supplemental Guidance Increasing the diversity of technologies within the Smart Grid information system reduces the impact from the exploitation of a specific technology. Requirement Enhancements None. Additional Considerations --	SG.SC-27.1 Determine if the organization employs diverse technologies in the implementation of the Smart Grid information system.	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; list of technologies deployed in the Smart Grid information system; acquisition documentation; acquisition contracts for Smart Grid information system components or services; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system acquisition, development, and implementation responsibilities].
SG.SC-28	Virtualization Technique	Tech	Category: Unique Technical Requirements Requirement The organization employs virtualization techniques to present gateway components into Smart Grid information system environments as other types of components, or components with differing configurations. Supplemental Guidance Virtualization techniques provide organizations with the ability to disguise gateway components into Smart Grid information system environments, potentially reducing the likelihood of successful attacks without the cost of having multiple platforms. Requirement Enhancements None. Additional Considerations A1. The organization employs virtualization techniques to deploy a diversity of operating systems environments and applications; A2. The organization changes the diversity of operating systems and applications on an organization-defined frequency; and A3. The organization employs randomness in the implementation of the virtualization.	SG.SC-28.1 Determine if the organization employs virtualization techniques to present gateway components into Smart Grid information system environments as other types of components, or components with differing configurations.	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system architecture; list of virtualization techniques to be employed for organizational Smart Grid information systems; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with responsibilities for implementing approved virtualization techniques for Smart Grid information systems].
SG.SC-29	Application Partitioning	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system separates user functionality (including user interface services) from Smart Grid information system management functionality. Supplemental Guidance Smart Grid information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from Smart Grid information system management functionality is either physical or logical. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system prevents the presentation of Smart Grid information system management-related functionality at an interface for general (i.e., non-privileged) users. Additional Considerations Supplemental Guidance The intent of this additional consideration is to ensure that administration options are not available to general users. For example, administration options are not presented until the user has appropriately established a session with administrator privileges.	SG.SC-29.1 Determine if the Smart Grid information system separates user functionality (including user interface services) from Smart Grid information system management functionality.	Examine, Test	Examine: [SELECT FROM: System and communications protection policy; procedures addressing application partitioning; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Test: [SELECT FROM: Separation of user functionality from Smart Grid information system management functionality].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SC-30	Information System Partitioning	Tech	Category: Common Technical Requirements, Integrity Requirement The organization partitions the Smart Grid information system into components residing in separate physical or logical domains (or environments). Supplemental Guidance An organizational assessment of risk guides the partitioning of Smart Grid information system components into separate domains (or environments). Requirement Enhancements None. Additional Considerations	SG.SC-30.1 Determine if the organization partitions the Smart Grid information system into components residing in separate physical or logical domains (or environments).	Examine, Interview	Examine: [SELECT FROM: System and communications protection policy; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; Smart Grid information system architecture; list of Smart Grid information system physical domains (or environments); Smart Grid information system facility diagrams; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel installing, configuring, and / or maintaining the Smart Grid information system].
				Smart Grid Information System and Information Integrity (SG.SI)		
SG.SI-1	System and Information Integrity Policy and Procedures	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization develops, implements, reviews, and updates on an organization-defined frequency— a. A documented Smart Grid information system and information integrity security policy that addresses— i. The objectives, roles, and responsibilities for the Smart Grid information system and information integrity security program as it relates to protecting the organization's personnel and assets; and ii. The scope of the Smart Grid information system and information integrity security program as it applies to all of the organizational staff, contractors, and third parties; and b. Procedures to address the implementation of the Smart Grid information system and information integrity security policy and associated Smart Grid information system and information integrity protection requirements; 2. Management commitment ensures compliance with the organization's security policy and other regulatory requirements; and 3. The organization ensures that the Smart Grid information system and information integrity policy and procedures comply with applicable federal, state, local, tribal, and territorial laws and regulations. Supplemental Guidance The Smart Grid information system and information integrity policy can be included as part of the general control security policy for the organization. Smart Grid information system and information integrity procedures can be developed for the security program in general and for a particular Smart Grid information system when required. Requirement Enhancements None. Additional Considerations None.	SG.SI-1.1 Determine if: (i) the organization develops and implements a documented Smart Grid information and integrity policy; (ii) the Smart Grid information and integrity policy addresses Smart Grid information and integrity as it related to protecting the organization's personnel and assets and the following: a) purpose / objective b) scope c) roles and responsibilities d) coordination among organizational entities, and compliance; (iii) the Smart Grid information and integrity policy addresses the scope to include all organizational staff, contractors, and third parties; (iv) the organization develops and implements the Smart Grid information and integrity procedures; (v) the organization reviews and updates the Smart Grid information and integrity procedures; (vi) management commitment ensures compliance with the organization's access control; (vii) the Smart Grid information and integrity policy comply with applicable federal, state, local, tribal, and territorial laws and regulations; and (viii) the Smart Grid information and integrity procedures facilitate implementation of the Smart Grid information and integrity security policy. SG.SI-1.2 Determine if: (i) the organization defines the frequency of Smart Grid information and integrity policy and procedures reviews/updates; (ii) the organization reviews/updates the Smart Grid information and integrity policy and procedures in accordance with the organization-defined frequency.	Examine, Interview	Examine: [SELECT FROM: Specific policy, standards, procedures, forms, memos and other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with specific ownership and responsibilities].
SG.SI-2	Flaw Remediation	GRC	Category: Common Technical Requirements, Integrity Requirement The organization— 1. Identifies, reports, and corrects Smart Grid information system flaws; 2. Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational Smart Grid information systems before installation; and 3. Incorporates flaw remediation into the organizational configuration management process. Supplemental Guidance The organization identifies Smart Grid information systems containing software and firmware (including operating system software) affected by recently announced flaws (and potential vulnerabilities resulting from those flaws). Flaws discovered during security assessments, continuous monitoring, or under incident response activities also need to be addressed. Requirement Enhancements None. Additional Considerations A1. The organization centrally manages the flaw remediation process. Organizations consider the risk of employing automated flaw remediation processes on a Smart Grid information system; A2. The organization employs automated mechanisms on an organization-defined frequency and on demand to determine the state of Smart Grid information system components with regard to flaw remediation; and A3. The organization employs automated patch management tools to facilitate flaw remediation to organization-defined Smart Grid information system components.	SG.SI-2.1 Determine if: (i) the organization identifies Smart Grid information system flaws; (ii) the organization reports Smart Grid information system flaws; (iii) the organization corrects Smart Grid information system flaws. SG.SI-2.2 Determine if the organization tests software updates related to flaw remediation for effectiveness and potential side effects on organizational Smart Grid information systems before installation. SG.SI-2.3 Determine if the organization incorporates flaw remediation into the organizational configuration management process.	Examine, Interview, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing flaw remediation; list of flaws and vulnerabilities potentially affecting the Smart Grid information system; list of recent security flaw remediation actions performed on the Smart Grid information system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct Smart Grid information system flaws); test results from the installation of software to correct Smart Grid information system flaws; Automated mechanisms supporting centralized management of flaw remediation and automatic software updates; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; list of Smart Grid information system flaws; list of recent security flaw remediation actions performed on the Smart Grid information system; Smart Grid information system audit records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with flaw remediation responsibilities]. Test: [SELECT FROM: Automated mechanisms supporting centralized management of flaw remediation and automatic software updates; Automated mechanisms implementing Smart Grid information system flaw remediation update status; Automated mechanisms facilitating flaw remediation to Smart Grid information system components].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SI-3	Malicious Code and Spam Protection	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization— a. Implements malicious code protection mechanisms; and b. Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures; and 2. The Smart Grid information system prevents users from circumventing malicious code protection capabilities. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization centrally manages malicious code protection mechanisms; A2. The Smart Grid information system updates malicious code protection mechanisms in accordance with organization-defined policies and procedures; A3. The organization configures malicious code protection methods to perform periodic scans of the Smart Grid information system on an organization-defined frequency; A4. The use of mechanisms to centrally manage malicious code protection must not degrade the operational performance of the Smart Grid information system; and A5. The organization employs spam protection mechanisms at system entry points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, Web accesses, or other common means.	SG.SI-3.1 Determine if: (i) the organization implements malicious code protection mechanisms; (ii) the organization updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures. SG.SI-3.2 Determine if the Smart Grid information system prevents users from circumventing malicious code protection capabilities.	Examine, Interview, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing malicious code protection; malicious code protection mechanisms; records of malicious code protection updates; procedures addressing spam protection; spam protection mechanisms; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with malicious code protection responsibilities; Organizational personnel with spam protection responsibilities]. Test: [SELECT FROM: Automated mechanisms implementing malicious code protection capability; Automated mechanisms implementing spam detection and handling capability].
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization monitors events on the Smart Grid information system to detect attacks, unauthorized activities or conditions, and non-malicious errors. Supplemental Guidance Smart Grid information system monitoring capability can be achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, log monitoring software, network monitoring software, and network forensic analysis tools). The granularity of the information collected can be determined by the organization based on its monitoring objectives and the capability of the Smart Grid information system to support such activities. Requirement Enhancements None. Additional Considerations A1. The Smart Grid information system notifies a defined list of incident response personnel; A2. The organization protects information obtained from intrusion monitoring tools from unauthorized access, modification, and deletion; A3. The organization tests/exercises intrusion monitoring tools on a defined time period; A4. The organization interconnects and configures individual intrusion detection tools into a Smart Grid system-wide intrusion detection system using common protocols; A5. The Smart Grid information system provides a real-time alert when indications of compromise or potential compromise occur; and A6. The Smart Grid information system prevents users from circumventing host-based intrusion detection and prevention capabilities.	SG.SI-4.1 Determine if the organization monitors events on the Smart Grid information system to detect attacks, unauthorized activities or conditions, and non-malicious errors.	Examine, Interview, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing Smart Grid information system monitoring tools and techniques; Smart Grid information system design documentation; Smart Grid information system monitoring tools and techniques documentation; Smart Grid information system configuration settings and associated documentation; techniques; documentation providing evidence of testing intrusion monitoring tools; Smart Grid information system monitoring tools and techniques documentation; list of common traffic patterns and / or events; Smart Grid information system protocols documentation; list of acceptable thresholds for false positives and false negatives; event correlation logs or records; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with Smart Grid information system monitoring responsibilities]. Test: [SELECT FROM: Smart Grid information system-wide intrusion detection capability; Automated tools supporting near real-time event analysis; Automated tools supporting the integration of intrusion detection tools and access/flow control mechanisms; Smart Grid information system monitoring real-time alert capability; Smart Grid information system-wide intrusion detection and prevention capability; Smart Grid information system notification capability; Automated mechanisms implementing alerts to security personnel for inappropriate or unusual activities; Automated mechanisms implementing wireless communications intrusion detection capability].
SG.SI-5	Security Alerts and Advisories	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement The organization— 1. Receives Smart Grid information system security alerts, advisories, and directives from external organizations; and 2. Generates and disseminates internal security alerts, advisories, and directives as deemed necessary. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization employs automated mechanisms to disseminate security alert and advisory information throughout the organization.	SG.SI-5.1 Determine if the organization receives Smart Grid information system security alerts, advisories, and directives from external organizations. SG.SI-5.2 Determine if: (i) the organization generates internal security alerts, advisories, and directives as deemed necessary; (ii) the organization disseminates internal security alerts, advisories, and directives as deemed necessary.	Examine, Interview, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing security alerts and advisories; records of security alerts and advisories; ; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; automated mechanisms supporting the distribution of security alert and advisory information; records of security alerts and advisories; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security alert and advisory responsibilities; organizational personnel implementing, operating, maintaining, administering, and using the Smart Grid information system]. Test: [SELECT FROM: Automated mechanisms implementing the distribution of security alert and advisory information].

Smart Grid Cyber Security Requirement		Req. Type	NISTIR 7628 Requirements Detail	Assessment Objective	Assessment Method	Potential Assessment Object(s)
SG.SI-6	Security Functionality Verification	GRC	Category: Common Governance, Risk, and Compliance (GRC) Requirements Requirement 1. The organization verifies the correct operation of security functions within the Smart Grid information system upon— a. Smart Grid information system startup and restart; and b. Command by user with appropriate privilege at an organization-defined frequency; and 2. The Smart Grid information system notifies the management authority when anomalies are discovered. Supplemental Guidance None. Requirement Enhancements None. Additional Considerations A1. The organization employs automated mechanisms to provide notification of failed automated security tests; and A2. The organization employs automated mechanisms to support management of distributed security testing.	SG.SI-6.1 Determine if the organization verifies the correct operation of security functions within the Smart Grid information system upon— a. Smart Grid information system startup and restart; and b. Command by user with appropriate privilege at an organization-defined frequency. SG.SI-6.2 Determine if the Smart Grid information system notifies the management authority when anomalies are discovered.	Examine, Interview, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing security function verification; Smart Grid information system design documentation; security plan; Smart Grid information system configuration settings and associated documentation; automated security test results; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security functionality verification responsibilities; organizational personnel with information security responsibilities]. Test: [SELECT FROM: Security function verification capability; Automated mechanisms implementing alerts and / or notifications for failed automated security tests; mated mechanisms supporting the management of distributed security function testing].
SG.SI-7	Software and Information Integrity	Tech	Category: Unique Technical Requirements Requirement The Smart Grid information system monitors and detects unauthorized changes to software and information. Supplemental Guidance The organization employs integrity verification techniques on the Smart Grid information system to look for evidence of information tampering, errors, and/or omissions. Requirement Enhancements 1. The organization reassesses the integrity of software and information by performing on an organization-defined frequency integrity scans of the Smart Grid information system. Additional Considerations A1. The organization employs centrally managed integrity verification tools; and A2. The organization employs automated tools that provide notification to designated individuals upon discovering	SG.SI-7.1 Determine if: (i) the Smart Grid information system monitors unauthorized changes to software and information; (ii) the Smart Grid information system detects unauthorized changes to software and information. SG.SI-7.2 (Requirement enhancement 1) Determine if: (i) the organization reassesses the integrity of software by performing on an organization-defined frequency integrity scans of the Smart Grid information system; (ii) the organization reassesses the integrity of information by performing on an organization-defined frequency integrity scans of the Smart Grid information system; (iii) the organization defines the frequency of the integrity scans of the Smart Grid information systems.	Examine, Interview, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing software and information integrity; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; integrity verification tools and applications documentation; automated tools supporting alerts and notifications for integrity discrepancies; records of integrity scans; Smart Grid information system component packaging; other relevant documents or records]. Interview: [SELECT FROM: Organizational personnel with security functionality verification responsibilities; organizational personnel with software integrity responsibilities; organization responsibility with change management responsibilities; organizational personnel with information security responsibilities]. Test: [SELECT FROM: Software integrity protection and verification capability].
SG.SI-8	Information Input Validation	Tech	Category: Common Technical Requirements, Integrity Requirement The Smart Grid information system employs mechanisms to check information for accuracy, completeness, validity, and authenticity. Supplemental Guidance Rules for checking the valid syntax of Smart Grid information system input (e.g., character set, length, numerical range, acceptable values) are in place to ensure that inputs match specified definitions for format and content. Requirement Enhancements None. Additional Considerations	SG.SI-8.1 Determine if: (i) the Smart Grid information system employs mechanisms to check information for accuracy; (ii) the Smart Grid information system employs mechanisms to check information for completeness; (iii) the Smart Grid information system employs mechanisms to check information for validity; (iv) the Smart Grid information system employs mechanisms to check information for authenticity.	Examine, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing information validity; access control policy and procedures; separation of duties policy and procedures; documentation for automated tools and applications to verify validity of information; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Test: [SELECT FROM: Smart Grid information system capability for checking validity of information inputs].
SG.SI-9	Error Handling	Tech	Category: Common Technical Requirements, Integrity Requirement The Smart Grid information system— 1. Identifies error conditions; and 2. Generates error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries. Supplemental Guidance The extent to which the Smart Grid information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. Requirement Enhancements None. Additional Considerations	SG.SI-9.1 Determine if the Smart Grid information system identifies error conditions. SG.SI-9.2 Determine if the Smart Grid information system generates error messages that provide information necessary for corrective actions without revealing potentially harmful information that could be exploited by adversaries.	Examine, Test	Examine: [SELECT FROM: System and information integrity policy; procedures addressing Smart Grid information system error handling; Smart Grid information system design documentation; Smart Grid information system configuration settings and associated documentation; other relevant documents or records]. Test: [SELECT FROM: Smart Grid information system error handling capability].

Cell: A1
Comment: Sandy Bacik:
Column: Smart Grid Cyber Security Requirement

This is based upon the NISTIR 7628 version 1.0 and shall not be modified.

Cell: C1
Comment: Sandy Bacik:
Column: Req. Type

This is based upon the NISTIR 7628 version 1.0 and shall not be modified.

Unique or Common Technical or Common Governance, Risk and Compliance (GRC).

Cell: D1
Comment: Sandy Bacik:
Column: NISTIR 7628 Requirements Detail

This is based upon the NISTIR 7628 version 1.0 and shall not be modified.

Cell: E1
Comment: Sandy Bacik:
Column: Assurance Objective

Based on assessment objectives in NIST SP800-53A (July 2008) - SP800-53A-final-sz.pdf and NIST SP800-53A Revision 1 (June 2010) - SP800-53A-rev1-final.pdf mapped to the NISTIR 7628 high level security requirements.

Cell: F1
Comment: Sandy Bacik:
Assessment methods define the nature of the assessor actions and include examine, interview, and test.

- The examine method is the process of reviewing, inspecting, observing, studying, or analyzing one or more assessment objects (i.e., specifications, mechanisms, or activities). The purpose of the examine method is to facilitate assessor understanding, achieve clarification, or obtain evidence.
- The interview method is the process of holding discussions with individuals or groups of individuals within an organization to once again, facilitate assessor understanding, achieve clarification, or obtain evidence.
- The test method is the process of exercising one or more assessment objects (i.e., activities or mechanisms) under specified conditions to compare actual with expected behavior.

In all three assessment methods, the results are used in making specific determinations called for in the determination statements and thereby achieving the objectives for the assessment procedure.

Cell: G1
Comment: Sandy Bacik:
Assessment objects identify the specific items being assessed and include specifications, mechanisms, activities, and individuals.

- Specifications are the document-based artifacts (e.g., policies, procedures, plans, system security requirements, functional specifications, and architectural designs) associated with an information system.
- Mechanisms are the specific hardware, software, or firmware safeguards and countermeasures employed within an information system.
- Activities are the specific protection-related pursuits or actions supporting an information system that involve people (e.g., conducting system backup operations, monitoring network traffic, exercising a contingency plan).
- Individuals, or groups of individuals, are people applying the specifications, mechanisms, or activities described above.

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security:		NERC CIPS (1-9) May 2009	AMI Security Requirements v2.0	
Access Control (SG.AC)								
SG.AC-1	Access Control Policy and Procedures	AC-1	Access Control Policy and Procedures	2.15.1	Access Control Policies and Procedures	CIP 003-2 (R1, R1.1, R1.3, R5, R5.3)	2.15.1	Access Control Policies and Procedures
SG.AC-2	Remote Access Policy and Procedures	AC-17	Remote Access	2.15.23	Remote Access Policy and Procedures	CIP005-2 (R1, R1.1, R1.2, R2, R2.3, R2.4)		
SG.AC-3	Account Management	AC-2	Account Management	2.15.3	Account Management	CIP 003-2 (R5, R5.1, R5.2, R5.3) CIP 004-2 (R4, R4.1, R4.2) CIP 005-2 (R2.5) CIP 007-2 (R5, R5.1, R5.2)	2.15.3	Account Management
SG.AC-4	Access Enforcement	AC-3	Access Enforcement	2.15.7	Access Enforcement	CIP 004-2 (R4) CIP 005-2 (R2, R2.1-R2.4)	2.15.7	Access Enforcement
SG.AC-5	Information Flow Enforcement	AC-4	Information Flow Enforcement	2.15.15	Information Flow Enforcement		2.15.15	Information Flow Enforcement
SG.AC-6	Separation of Duties	AC-5	Separation of Duties	2.15.8	Separation of Duties		2.15.8	Separation of Duties
SG.AC-7	Least Privilege	AC-6	Least Privilege	2.15.9	Least Privilege	CIP 007-2 (R5.1)	2.15.9	Least Privilege
SG.AC-8	Unsuccessful Login Attempts	AC-7	Unsuccessful Login Attempts	2.15.20	Unsuccessful Logon Notification		2.15.20	Unsuccessful Logon Notification
SG.AC-9	Smart Grid Information System Use Notification	AC-8	System Use Notification	2.15.17	System Use Notification	CIP 005-2 (R2.6)	2.15.17	System Use Notification
SG.AC-10	Previous Logon Notification	AC-9	Previous Logon (Access) Notification	2.15.19	Previous Logon Notification		2.15.19	Previous Logon Notification
SG.AC-11	Concurrent Session Control	AC-10	Concurrent Session Control	2.15.18	Concurrent Session Control		2.15.18	Concurrent Session Control
SG.AC-12	Session Lock	AC-11	Session Lock	2.15.21	Session Lock		2.15.21	Session Lock
SG.AC-13	Remote Session Termination			2.15.22	Remote Session Termination		2.15.22	Remote Session Termination
SG.AC-14	Permitted Actions without Identification or Authentication	AC-14	Permitted Actions without Identification or Authentication	2.15.11	Permitted Actions without Identification and Authentication		2.15.11	Permitted Actions without Identification and Authentication
SG.AC-15	Remote Access	AC-17	Remote Access	2.15.24	Remote Access	CIP 005-2 (R2, R3, R3.1, R3.2)	2.15.24	Remote Access
SG.AC-16	Wireless Access Restrictions			2.15.26	Wireless Access Restrictions		2.15.26	Wireless Access Restrictions
SG.AC-17	Access Control for Portable and Mobile Devices	AC-19	Access Control for Mobile Devices	2.15.25	Access Control for Portable and Mobile Devices	CIP 005-2 (R2.4, R5, R5.1)	2.15.25	Access Control for Portable and Mobile Devices
SG.AC-18	Use of External Information Control Systems	SC-7	Boundary Protection	2.15.29	Use of External Information Control Systems		2.15.29	Use of External Information Control Systems
SG.AC-19	Control System Access Restrictions			2.15.28	External Access Protections		2.15.28	External Access Protections
SG.AC-20	Publicly Accessible Content							
SG.AC-21	Passwords			2.15.16	Passwords	CIP 007-2 (R5.3)	2.15.16	Passwords
Awareness and Training (SG.AT)								

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security:		NERC CIPS (1-9) May 2009	AMI Security Requirements v2.0	
SG.AT-1	Awareness and Training Policy and Procedures	AT-1	Security Awareness and Training Policy and Procedures	2.11.1	Security Awareness Training Policy and Procedures	CIP 004-2 (R1, R2)		
SG.AT-2	Security Awareness	AT-2	Security Awareness	2.11.2	Security Awareness	CIP 004-2 (R1)		
SG.AT-3	Security Training	AT-3	Security Training	2.11.3	Security Training	CIP 004-2 (R2)		
SG.AT-4	Security Awareness and Training Records	AT-4	Security Training Records	2.11.4	Security Training Records	CIP 004-2 (R2.3)		
SG.AT-5	Contact with Security Groups and Associations	AT-5	Contact with Security Groups and Associations	2.11.5	Contact with Security Groups and Associations			
SG.AT-6	Security Responsibility Training			2.11.6	Security Responsibility Training			
SG.AT-7	Planning Process Training			2.7.5	Planning Process Training	CIP 004-2 (R2)		
Audit and Accountability (SG.AU)								
SG.AU-1	Audit and Accountability	AU-1	Audit and Accountability Policy and Procedures	2.16.1	Audit and Accountability Process and Procedures	CIP 003-2 (R1, R1.1, R1.3)		
SG.AU-2	Auditable Events	AU-2	Auditable Events	2.16.2	Auditable Events	CIP 005-2 (R1, R1.1, R1.3)	2.16.2	Auditable Events
		AU-13	Monitoring for Information Disclosure			CIP 007-2 (R5.1.2, R5.2.3, R6.1, R6.3)		
SG.AU-3	Content of Audit Records	AU-3	Content of Audit Records	2.16.3	Content of Audit Records	CIP 007-3 (R5.1.2)	2.16.3	Content of Audit Records
SG.AU-4	Audit Storage Capacity	AU-4	Audit Storage Capacity	2.16.4	Audit Storage		2.16.4	Audit Storage
SG.AU-5	Response to Audit Processing Failures	AU-5	Response to Audit Processing Failures	2.16.5	Response to Audit Processing Failures		2.16.5	Response to Audit Processing Failures
SG.AU-6	Audit Monitoring, Analysis, and Reporting	AU-6	Audit Monitoring, Analysis, and Reporting	2.16.6	Audit Monitoring, Process, and Reporting	CIP 007-2 (R5.1.2)		
						CIP 007-2 (R6.5)		
SG.AU-7	Audit Reduction and Report Generation	AU-7	Audit Reduction and Report Generation	2.16.7	Audit Reduction and Report Generation		2.16.7	Audit Reduction and Report Generation
SG.AU-8	Time Stamps	AU-8	Time Stamps	2.16.8	Time Stamps		2.16.8	Time Stamps
SG.AU-9	Protection of Audit Information	AU-9	Protection of Audit Information	2.16.9	Protection of Audit Information	CIP 003-2 (R4)	2.16.9	Protection of Audit Information
SG.AU-10	Audit Record Retention	AU-11	Audit Record Retention	2.16.10	Audit Record Retention	CIP 005-2 (R5.3)		
						CIP 007-2 (R5.1.2, R6.4)		
						CIP 008-2 (R2)		
SG.AU-11	Conduct and Frequency of Audits	AU-1	Audit and Accountability Policy and Procedures	2.16.11	Conduct and Frequency of Audits			
SG.AU-12	Auditor Qualification			2.16.12	Auditor Qualification		2.16.12	Auditor Qualification
SG.AU-13	Audit Tools	AU-7	Audit Reduction and Report Generation	2.16.13	Audit Tools		2.16.13	Audit Tools
SG.AU-14	Security Policy Compliance	CA-1	Security Assessment and Authorization Policies and Procedures	2.16.14	Security Policy Compliance			
SG.AU-15	Audit Generation	AU-12	Audit Generation	2.16.15	Audit Generation			
SG.AU-16	Non-Repudiation	AU-10	Non-Repudiation	2.16.16	Non-Repudiation			
Security Assessment and Authorization (SG.CA)								
SG.CA-1	Security Assessment and Authorization Policy and Procedures	CA-1	Security Assessment and Authorization Policies and Procedures	2.18.3	Certification, Accreditation, and Security Assessment Policies and Procedures		2.18.3	Certification, Accreditation, and Security Assessment Policies and Procedures

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security:		NERC CIPS (1-9) May 2009	AMI Security Requirements v2.0	
				2.17.1	Monitoring and Reviewing Control System Security management Policy and Procedures		2.17.1	Monitoring and Reviewing Control System Security management Policy and Procedures
SG.CA-2	Security Assessments	CA-2	Security Assessments	2.17.3	Monitoring of Security Policy		2.17.3	Monitoring of Security Policy
SG.CA-3	Continuous Improvement			2.17.2	Continuous Improvement		2.17.2	Continuous Improvement Best Practices
				2.17.4	Best Practices		2.17.4	Continuous Improvement Best Practices
SG.CA-4	Information System Connections	CA-3	Information System Connection	2.18.5	Control System Connections	CIP 005-2 (R2)	2.18.5	Control System Connections
SG.CA-5	Security Authorization to Operate	CA-6	Security Authorization	2.17.5	Security Accreditation		2.17.5	Security Accreditation
		PM-10	Security Authorization Process					
SG.CA-6	Continuous Monitoring	CA-7	Continuous Monitoring	2.18.7	Continuous Monitoring		2.18.7	Continuous Monitoring
Configuration Management (SG.CM)								
SG.CM-1	Configuration Management Policy and Procedures	CM-1	Configuration Management Policy and Procedures	2.6.1	Configuration Management Policy and Procedures	CIP 003-2 (R6)		
SG.CM-2	Baseline Configuration	CM-2	Baseline Configuration	2.6.2	Baseline Configuration	CIP 007-2 (R9)		
SG.CM-3	Configuration Change Control	CM-3	Configuration Change Control	2.6.3	Configuration Change Control	CIP 003-2 (R6)		
		SA-10	Developer Configuration Management					
SG.CM-4	Monitoring Configuration Changes	CM-4	Security Impact Analysis	2.6.4	Monitoring Configuration Changes	CIP 003-2 (R6)		
		SA-10	Developer Configuration Management					
SG.CM-5	Access Restrictions for Configuration Change	CM-5	Access Restrictions for Change	2.6.5	Access Restrictions for Configuration Change	CIP 003-2 (R6)		
SG.CM-6	Configuration Settings	CM-6	Configuration Settings	2.6.6	Configuration Settings	CIP 003-2 (R6)		
						CIP 005 (R2.2)		
SG.CM-7	Configuration for Least Functionality	CM-7	Least Functionality	2.6.7	Configuration for Least Functionality			
SG.CM-8	Component Inventory	CM-8	Information System Component Inventory	2.6.8	Configuration Assets			
SG.CM-9	Addition, Removal, and Disposal of Equipment	MP-6	Media Sanitization	2.6.9	Addition, Removal, and Disposition of Equipment	CIP 003-2 (R6)		
SG.CM-10	Factory Default Settings Management			2.6.10	Factory Default Authentication Management	CIP 005-2 (R4.4)		
SG.CM-11	Configuration Management Plan	CM-9	Configuration Management Plan					
Continuity of Operations (SG.CP)								
SG.CP-1	Continuity of Operations Policy and Procedures	CP-1	Contingency Planning Policy and Procedures					
SG.CP-2	Continuity of Operations Plan	CP-1	Contingency Planning Policy and Procedures	2.12.2	Continuity of Operations Plan	CIP 008-2 (R1)	2.12.2	Continuity of Operations Plan
						CIP 009-2 (R1)		
SG.CP-3	Continuity of Operations Roles and Responsibilities	CP-2	Contingency Plan	2.12.3	Continuity of Operations Roles and Responsibilities	CIP 009-2 (R1.1, R1.2)	2.12.3	Continuity of Operations Roles and Responsibilities
SG.CP-4	Continuity of Operations Training							
SG.CP-5	Continuity of Operations Plan Testing	CP-4	Contingency Plan Testing and Exercises	2.12.5	Continuity of Operations Plan Testing	CIP 008-2 (R1.6)	2.12.5	Continuity of Operations Plan Testing
						CIP 009-2 (R2, R5)		

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security:		NERC CIPS (1-9) May 2009	AMI Security Requirements v2.0	
SG.CP-6	Continuity of Operations Plan Update			2.12.6	Continuity of Operations Plan Update	CIP 009-2 (R4, R5)	2.12.6	Continuity of Operations Plan Update
SG.CP-7	Alternate Storage Sites	CP-6	Alternate Storage Sites	2.12.13	Alternative Storage Sites			
SG.CP-8	Alternate Telecommunication Services	CP-8	Telecommunications Services	2.12.14	Alternate Command/Control Methods			
SG.CP-9	Alternate Control Center	CP-7	Alternate Processing Site	2.12.15	Alternate Control Center			
		CP-8	Telecommunications Services					
SG.CP-10	Smart Grid Information System Recovery and Reconstitution	CP-10	Information System Recovery and Reconstitution	2.12.17	Control System Recovery and Reconstitution	CIP 009-2 (R4)		
SG.CP-11	Fail-Safe Response			2.12.18	Fail-Safe Response			
Identification and Authentication (SG.IA)								
SG.IA-1	Identification and Authentication Policy and Procedures	IA-1	Identification and Authentication Policy and Procedures	2.15.2	Identification and Authentication Procedures and Policy		2.15.2	Identification and Authentication Procedures and Policy
SG.IA-2	Identifier Management	IA-4	Identifier Management	2.15.4	Identifier Management		2.15.4	Identifier Management
SG.IA-3	Authenticator Management	IA-5	Authenticator Management	2.15.5	Authenticator Management	CIP 007-2 (R5, R5.1, R5.2, R5.3)	2.15.5	Authenticator Management
SG.IA-4	User Identification and Authentication	IA-2	User Identification and Authentication	2.15.10	User Identification and Authentication	CIP 003-2 (R1, R1.1, R1.3)	2.15.10	User Identification and Authentication
SG.IA-5	Device Identification and Authentication	IA-3	Device Identification and Authentication	2.15.12	Device Authentication and Identification		2.15.12	Device Authentication and Identification
SG.IA-6	Authenticator Feedback	IA-6	Authenticator Feedback	2.15.13	Authenticator Feedback		2.15.13	Authenticator Feedback
Information and Document Management (SG.ID)								
SG.ID-1	Information and Document Management Policy and Procedures			2.9.1	Information and Document Management Policy and Procedures		2.9.1	Information and Document Management Policy and Procedures
SG.ID-2	Information and Document Retention			2.9.2	Information and Document Retention	CIP 006-2 (R7)	2.9.2	Information and Document Retention
SG.ID-3	Information Handling	MP-1	Media Protection Policy and Procedures	2.9.3	Information Handling	CIP 003-2 (R4.1)	2.9.3	Information Handling
SG.ID-4	Information Exchange			2.9.5	Information Exchange		2.9.5	Information Exchange
SG.ID-5	Automated Labeling			2.9.11	Automated Labeling			
Incident Response (SG.IR)								
SG.IR-1	Incident Response Policy and Procedures	IR-1	Incident Response Policy and Procedures	2.12.1	Incident Response Policy and Procedures		2.12.1	Incident Response Policy and Procedures
SG.IR-2	Incident Response Roles and Responsibilities	IR-1	Incident Response Policy and Procedures	2.7.4	Roles and Responsibilities	CIP 008-2 (Rr1.2) CIP 009-2 (R1.2)		
SG.IR-3	Incident Response Training	IR-2	Incident Response Training	2.12.4	Incident Response Training		2.12.4	Incident Response Training
SG.IR-4	Incident Response Testing and Exercises	IR-3	Incident Response Testing and Exercises					
SG.IR-5	Incident Handling	IR-4	Incident Handling	2.12.7	Incident Handling			
SG.IR-6	Incident Monitoring	IR-5	Incident Monitoring	2.12.8	Incident Monitoring			
SG.IR-7	Incident Reporting	IR-6	Incident Reporting	2.12.9	Incident Reporting			

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security:		NERC CIPS (1-9) May 2009	AMI Security Requirements v2.0	
SG.IR-8	Incident Response Investigation and Analysis	PE-6	Monitoring Physical Access	2.12.11	Incident Response Investigation and Analysis	CIP 008-2 (R1, R1.2-R1.5)		
SG.IR-9	Corrective Action			2.12.12	Corrective Action	CIP 008-2 (R1.4) CIP 009-2 (R3)		
SG.IR-10	Smart Grid Information System Backup	CP-9	Information System Backup	2.12.16	Control System Backup			
SG.IR-11	Coordination of Emergency Response			2.2.4	Coordination of Threat Mitigation	CIP 008-2 (R1.3)		
Smart Grid Information System Development and Maintenance (SG.MA)								
SG.MA-1	Smart Grid Information System Maintenance Policy and Procedures	MA-1	System Maintenance Policy and Procedures	2.10.1	System Maintenance Policy and Procedures		2.10.1	System Maintenance Policy and Procedures
SG.MA-2	Legacy Smart Grid Information System Updates			2.10.2	Legacy System Upgrades		2.10.2	Legacy System Upgrades
SG.MA-3	Smart Grid Information System Maintenance	PL-6	Security-Related Activity Planning	2.10.5	Unplanned System Maintenance		2.10.5	Unplanned System Maintenance
		MA-2	Controlled Maintenance	2.10.6	Periodic System Maintenance		2.10.6	Periodic System Maintenance
SG.MA-4	Maintenance Tools	MA-3	Maintenance Tools	2.10.7	Maintenance Tools		2.10.7	Maintenance Tools
SG.MA-5	Maintenance Personnel	MA-5	Maintenance Personnel	2.10.8	Maintenance Personnel		2.10.8	Maintenance Personnel
SG.MA-6	Remote Maintenance	MA-4	Non-Local Maintenance	2.10.9	Remote Maintenance		2.10.9	Remote Maintenance
SG.MA-7	Timely Maintenance	MA-6	Timely Maintenance	2.10.10	Timely Maintenance	CIP 009-2 (R4)		
Media Protection (SG.MP)								
SG.MP-1	Media Protection Policy and Procedures	MP-1	Media Protection Policy and Procedures	2.13.1	Media Protection and Procedures			
SG.MP-2	Media Sensitivity Level	RA-2	Security Categorization	2.13.3	Media Classification	CIP 003-2 (R4, R4.2)	2.9.4	Information Classification
				2.9.4	Information Classification			
SG.MP-3	Media Marketing	MP-3	Media Marketing	2.13.4	Media Labeling		2.9.10	Automated Marking
				2.9.10	Automated Marking			
SG.MP-4	Media Storage	MP-4	Media Storage	2.13.5	Media Storage			
SG.MP-5	Media Transport	MP-5	Media Transport	2.13.6	Media Transport			
SG.MP-6	Media Sanitization and Disposal	MP-6	Media Sanitization	2.13.7	Media Sanitization and Storage	CIP 007-2 (R7, R7.1, R7.2, R7.3)		
Physical and Environmental Security (SG.PE)								
SG.PE-1	Physical and Environmental Security Policy and Procedures	PE-1	Physical and Environmental Protection Policy and Procedures	2.4.1	Physical and Environmental Security Policies and Procedures	CIP 006-2 (R1, R2)		
SG.PE-2	Physical Access Authorizations	PE-2	Physical Access Authorizations	2.4.2	Physical Access Authorizations	CIP 004-2 (R4)		
SG.PE-3	Physical Access	PE-3	Physical Access Control	2.4.3	Physical Access Control	CIP 006-2 (R2)		
		PE-4	Access Control for Transmission Medium					
		PE-5	Access Control for Output Devices					
SG.PE-4	Monitoring Physical Access	PE-6	Monitoring Physical Access	2.4.4	Monitoring Physical Access	CIP 006-2 (R5)		
SG.PE-5	Visitor Control	PE-7	Visitor Control	2.4.5	Visitor Control	CIP 006-2 (R1.4)		
SG.PE-6	Visitor Records	PE-8	Access Records	2.4.6	Visitor Records	CIP 006-2 (R1.4, R6)		
SG.PE-7	Physical Access Log Retention			2.4.7	Physical Access Log Retention	CIP 006-2 (R7)		
SG.PE-8	Emergency Shutoff Protection	PE-10	Emergency Shutoff	2.4.8	Emergency Shutoff			
SG.PE-9	Emergency Power	PE-11	Emergency Power	2.4.9	Emergency Power			
SG.PE-10	Delivery and Removal	PE-16	Delivery and Removal	2.4.14	Delivery and Removal			
SG.PE-11	Alternate Work Site	PE-17	Alternate Work Site	2.4.15	Alternate Work Site			

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security:		NERC CIPS (1-9) May 2009	AMI Security Requirements v2.0	
SG.PE-12	Location of Smart Grid Information System Assets	PE-18	Location of Information System Components	2.4.18	Location of Control System Assets			
Planning (SG.PL)								
SG.PL-1	Strategic Planning Policy and Procedures	PL-1	Security Planning and Procedures	2.7.1	Strategic Planning Policy and Procedures			
SG.PL-2	Smart Grid Information System Security Plan	PL-2	System Security Plan	2.7.2	Control System Security Plan			
SG.PL-3	Rules of Behavior	PL-4	Rules of Behavior	2.7.11	Rules of Behavior			
SG.PL-4	Privacy Impact Assessment	PL-5	Privacy Impact Assessment					
SG.PL-5	Security-Related Activity Planning	PL-6	Security-Related Activity Planning	2.7.12	Security-Related Activity Planning	CIP 002-2 (R1)		
Security Program Management (SG.PM)								
SG.PM-1	Security Policy and Procedures	AC-1	Access Control Policy and Procedures	2.1.1	Security Policies and Procedures	CIP 003-2 (R1, R1.1, R1.3, R5, R5.3)		
SG.PM-2	Security Program Plan	PM-1	Information Security Program Plan					
SG.PM-3	Senior Management Authority	PM-2	Senior Information Security Officer					
SG.PM-4	Security Architecture	PM-7	Enterprise Architecture					
SG.PM-5	Risk Management Strategy	PM-9	Risk Management Strategy					
SG.PM-6	Security Authorization to Operate Process	PM-10	Security Authorization Process					
SG.PM-7	Mission/Business Process Definition	PM-11	Mission/Business Process Definition					
SG.PM-8	Management Accountability	PM-1	Information Security Program Plan	2.2.2	Management Accountability	CIP 003-2 (R2, R3)		
Personnel Security (SG.PS)								
SG.PS-1	Personnel Security Policy and Procedures	PS-1	Personnel Security Policy and Procedures	2.3.1	Personnel Security Policies and Procedures	CIP 004-2 (R3)		
SG.PS-2	Position Categorization	PS-2	Position Categorization	2.3.2	Position Categorization	CIP 004-2 (R3)		
SG.PS-3	Personnel Screening	PS-3	Personnel Screening	2.3.3	Personnel Screening	CIP 004-2 (R3)		
SG.PS-4	Personnel Termination	PS-4	Personnel Termination	2.3.4	Personnel Termination	CIP 004-2 (R4.2) CIP 004-2 (R5.2.3)		
SG.PS-5	Personnel Transfer	PS-5	Personnel Transfer	2.3.5	Personnel Transfer	CIP 004-2 (R4.1, R4.2)		
SG.PS-6	Access Agreements	PS-6	Access Agreements	2.3.6	Access Agreements			
SG.PS-7	Contractor and Third-Party Personnel Security	PS-7	Third-Party Personnel Security	2.3.7	Third-Party Security Agreements	CIP 004-2 (R3.3)		
SG.PS-8	Personnel Accountability	PS-8	Personnel Sanctions	2.3.8	Personnel Accountability			
SG.PS-9	Personnel Roles			2.3.9	Personnel Roles			
Risk Management and Assessment (SG.RA)								
SG.RA-1	Risk Assessment Policy and Procedures	RA-1	Risk Assessment Policy and Procedures	2.18.1	Risk Assessment Policy and Procedures	CIP 002-2 (R1, R1.1, R1.2, R4) CIP 003-2 (R1, R4.2)		
SG.RA-2	Risk Management Plan	PM-9	Risk Management Strategy	2.18.2	Risk Management Plan	CIP 003-2 (R4, R4.1, R4.2)		
SG.RA-3	Security Impact Level	RA-2	Security Categorization	2.18.8	Security Categorization			
SG.RA-4	Risk Assessment	RA-3	Risk Assessment	2.18.9	Risk Assessment	CIP 002-2 (R1.2)		
SG.RA-5	Risk Assessment Update	RA-3	Risk Assessment	2.18.10	Risk Assessment Update	CIP 002-2 (R4)		
SG.RA-6	Vulnerability Assessment and Awareness	RA-5	Vulnerability Scanning	2.18.11	Vulnerability Assessment and Awareness	CIP 005-2 (R4, R4.2, R4.3, R4.4)		

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security:		NERC CIPS (1-9) May 2009	AMI Security Requirements v2.0	
						CIP 007-2 (R8)		
Smart Grid Information System and Services Acquisition (SG.SA)								
SG.SA-1	Smart Grid Information System and Services Acquisition Policy and Procedures	SA-1	System and Services Acquisition Policy and Procedures	2.5.1	System and Services Acquisition Policy and Procedures			
SG.SA-2	Security Policies for Contractors and Third Parties			2.2.5	Security Policies for Third Parties			
				2.2.6	Termination of Third-Party Access			
SG.SA-3	Life-Cycle Support	SA-3	Life-Cycle Support	2.5.3	Life-Cycle Support			
SG.SA-4	Acquisitions	SA-4	Acquisitions	2.5.4	Acquisitions			
SG.SA-5	Smart Grid Information System Documentation	SA-5	Information System Documentation	2.5.5	Control System Documentation			
SG.SA-6	Software License Usage Restrictions	SA-6	Software Usage Restrictions	2.5.6	Software License Usage Restrictions			
SG.SA-7	User-Installed Software	SA-7	User-Installed Software	2.5.7	User-installed Software			
SG.SA-8	Security Engineering Principles	SA-8	Security Engineering Principles	2.5.8	Security Engineering Principals			
		SA-13	Trustworthiness					
SG.SA-9	Developer Configuration Management	SA-10	Developer Configuration Management	2.5.10	Vendor Configuration Management			
SG.SA-10	Developer Security Testing	SA-11	Developer Security Testing	2.5.11	Vendor Security Testing			
SG.SA-11	Supply Chain Protection	SA-12	Supply Chain Protection	2.5.12	Vendor Life-cycle Practices			
Smart Grid Information System and Communication Protection (SG.SC)								
SG.SC-1	System and Communication Protection Policy and Procedures	SC-1	System and Communication Protection Policy and Procedures	2.8.1	System and Communication Protection Policy and Procedures	CIP 003-2 (R1, R1.1, R1.3)		
SG.SC-2	Communications Partitioning			2.8.2	Management Port Partitioning		2.8.2	Management Port Partitioning
SG.SC-3	Security Function Isolation	SC-3	Security Function Isolation	2.8.3	Security Function Isolation		2.8.3	Security Function Isolation
SG.SC-4	Information Remnants	SC-4	Information in Shared Resources	2.8.4	Information Remnants		2.8.4	Information Remnants
SG.SC-5	Denial-of-Service Protection	SC-5	Denial-of-Service Protection	2.8.5	Denial-of-Service Protection		2.8.5	Denial-of-Service Protection
SG.SC-6	Resource Priority	SC-6	Resource Priority	2.8.6	Resource Priority		2.8.6	Resource Priority
SG.SC-7	Boundary Protection	SC-7	Boundary Protection	2.8.7	Boundary Protection	CIP 005-2 (R1, R1.1, R1.2, R1.3, R1.4, R1.6, R2, R2.1-R2.4, R5, R5.1)	2.8.7	Boundary Protection
SG.SC-8	Communication Integrity	SC-8	Transmission Integrity	2.8.8	Communication Integrity		2.8.8	Communication Integrity
SG.SC-9	Communication Confidentiality	SC-9	Transmission Confidentiality	2.8.9	Communication Confidentially		2.8.9	Communication Confidentially
SG.SC-10	Trusted Path	SC-11	Trusted Path	2.8.10	Trusted Path		2.8.10	Trusted Path
SG.SC-11	Cryptographic Key Establishment and Management	SC-12	Cryptographic Key Establishment and Management	2.8.11	Cryptographic Key Establishment and Management		2.8.11	Cryptographic Key Establishment and Management
SG.SC-12	Use of Validated Cryptography	SC-13	Use of Cryptography	2.8.12	Use of Validated Cryptography		2.8.12	Use of Validated Cryptography
SG.SC-13	Collaborative Computing	SC-15	Collaborative Computing Devices	2.8.13	Collaborative Computing		2.8.13	Collaborative Computing
SG.SC-14	Transmission of Security Parameters	SC-16	Transmission of Security Attributes	2.8.14	Transmission of Security Parameters		2.8.14	Transmission of Security Parameters
SG.SC-15	Public Key Infrastructure Certificates	SC-17	Public Key Infrastructure Certificates	2.8.15	Public Key Infrastructure Certificates		2.8.15	Public Key Infrastructure Certificates
SG.SC-16	Mobile Code	SC-18	Mobile Code	2.8.16	Mobile Code		2.8.16	Mobile Code
SG.SC-17	Voice-Over Internet Protocol	SC-19	Voice Over Internet Protocol	2.8.17	Voice-over-Internet Protocol		2.8.17	Voice-over-Internet Protocol
SG.SC-18	System Connections	CA-3	Information System Connections	2.8.18	System Connections	CIP 005-2 (R2, R2.2-R2.4)	2.8.18	System Connections
SG.SC-19	Security Roles	SA-9	External Information System Services	2.8.19	Security Roles	CIP 003-2 (R5)	2.8.19	Security Roles

Smart Grid Cyber Security Requirement		NIST SP 800-53 Revision 3		DHS Catalog of Control Systems Security:		NERC CIPS (1-9) May 2009	AMI Security Requirements v2.0	
SG.SC-20	Message Authenticity	SC-8	Transmission Integrity	2.8.20	Message Authenticity		2.8.20	Message Authenticity
SG.SC-21	Secure Name/Address Resolution Service	SC-20	Secure Name/Address Resolution Service (Authoritative Source)	2.8.22	Secure Name/Address Resolution Service (Authoritative Source)		2.8.22	Secure Name/Address Resolution Service (Authoritative Source)
SG.SC-22	Fail in Known State	SC-24	Fail in Known State	2.8.24	Fail in Know State			
SG.SC-23	Thin Nodes	SC-25	Thin Nodes	2.8.25	Thin Nodes			
SG.SC-24	Honeypots	SC-26	Honeypots	2.8.26	Honeypots			
SG.SC-25	Operating System-Independent Applications	SC-27	Operating System-Independent Applications	2.8.27	Operating System-Independent Applications			
SG.SC-26	Confidentiality of Information at Rest	SC-28	Confidentiality of Information at Rest	2.8.28	Confidentiality of Information at Rest			
SG.SC-27	Heterogeneity	SC-29	Heterogeneity	2.8.29	Heterogeneity			
SG.SC-28	Virtualization Technique	SC-30	Virtualization Technique	2.8.30	Virtualization Techniques			
SG.SC-29	Application Partitioning			2.8.32	Application Partitioning			
SG.SC-30	Information System Partitioning	SC-32	Information Systems Partitioning					
Smart Grid Information System and Information Integrity (SG.SI)								
SG.SI-1	System and Information Integrity Policy and Procedures	SI-1	System and Information Integrity Policy and Procedures	2.14.1	System and Information Integrity Policy and Procedures		2.14.1	System and Information Integrity Policy and Procedures
SG.SI-2	Flaw Remediation	SI-2	Flaw Remediation	2.14.2	Flaw Remediation	CIP 007-2 (R3, R3.1, R3.2)	2.14.2	Flaw Remediation
SG.SI-3	Malicious Code and Spam Protection	SI-3	Malicious Code Protection	2.14.3	Malicious Code Protection	CIP 007-2 (R4, R4.1, R4.2)	2.14.3	Malicious Code Protection
		SI-8	Spam Protection	2.14.8	Spam Protection	CIP 007-2 (R4)		
SG.SI-4	Smart Grid Information System Monitoring Tools and Techniques	SI-4	Information System Monitoring	2.14.4	System Monitoring Tools and Techniques	CIP 007-2 (R6)	2.14.8	Spam Protection
SG.SI-5	Security Alerts and Advisories	SI-5	Security Alerts, Advisories, and Directives	2.14.5	Security Alerts and Advisories		2.14.4	System Monitoring Tools and Techniques
SG.SI-6	Security Functionality Verification	SI-6	Security Functionality Verification	2.14.6	Security Functionality Verification	CIP 007-2 (R1)	2.14.5	Security Alerts and Advisories
SG.SI-7	Software and Information Integrity	SI-7	Software and Information Integrity	2.14.7	Software and Information Integrity		2.14.6	Security Functionality Verification
SG.SI-8	Information Input Validation	SI-10	Information Input Validation	2.14.9	Information Input Restrictions	CIP 003-2 (R5)	2.14.7	Software and Information Integrity
				2.14.10	Information Input Accuracy, Completeness Validity and Authenticity	CIP 007-2 (R, R5.1, R5.2)	2.14.10	Information Input Accuracy, Completeness, Validity and Authenticity
SG.SI-9	Error Handling	SI-11	Error Handling	2.14.11	Error Handling		2.14.11	Error Handling

ASSESSMENT METHOD	ASSESSMENT OBJECTS	DEFINITION	SUPPLEMENTAL GUIDANCE	ATTRIBUTE: Depth	ATTRIBUTE: Coverage
Examine	Specifications (e.g., policies, plans, procedures, system requirements, designs) Mechanisms (e.g., functionality implemented in hardware, software, firmware) Activities (e.g., system operations, administration, management, exercises)	The process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence. The results are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.	Typical assessor actions may include, for example: • reviewing information security policies, plans, and procedures; • analyzing system design documentation and interface specifications; • observing system backup operations, reviewing the results of contingency plan exercises; • observing incident response activities; • studying technical manuals and user/administrator guides; • checking, studying, or observing the operation of an information technology mechanism in the Smart Grid information system hardware/software; or • checking, studying, or observing physical security measures related to the operation of a Smart Grid information system.	The depth attribute addresses the rigor of and level of detail in the examination process. There are three possible values for the depth attribute: (i) basic; (ii) focused; and (iii) comprehensive. • Basic examination: Examination that consists of high-level reviews, checks, observations, or inspections of the assessment object. This type of examination is conducted using a limited body of evidence or documentation (e.g., functional-level descriptions for mechanisms; high-level process descriptions for activities; and actual documents for specifications). Basic examinations provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors. • Focused examination: Examination that consists of high-level reviews, checks, observations, or inspections and more in depth studies/analyses of the assessment object. This type of examination is conducted using a substantial body of evidence or documentation (e.g., functional-level descriptions and where appropriate and available, high-level design information for mechanisms; high-level process descriptions and implementation procedures for activities; and the actual documents and related documents for specifications). Focused examinations provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended. • Comprehensive examination: Examination that consists of high-level reviews, checks, observations, or inspections and more in depth, detailed, and thorough studies/analyses of the assessment object. This type of examination is conducted using an extensive body of evidence or documentation (e.g., functional-level descriptions and where appropriate and available, high-level design information, low-level design information, and implementation information for mechanisms; high-level process descriptions and detailed implementation procedures for activities; and the actual documents and related documents for specifications44). Comprehensive examinations provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operatin as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.	The coverage attribute addresses the scope or breadth of the examination process and includes the types of assessment objects to be examined, the number of objects to be examined (by type), and specific objects to be examined.45 There are three possible values for the coverage attribute: (i) basic, (ii) focused, and (iii) comprehensive. • Basic examination: examination that uses a representative sample of assessment objects (by type and number within type) to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors. • Focused examination: examination that uses a representative sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended. • Comprehensive examination: examination that uses a sufficiently large sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.

ASSESSMENT METHOD	ASSESSMENT OBJECTS	DEFINITION	SUPPLEMENTAL GUIDANCE	ATTRIBUTE: Depth	ATTRIBUTE: Coverage
Interview	Individuals or groups of individuals.	The process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence. The results are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.	Typical assessor actions may include, for example: • interviewing agency heads, • chief information officers, • senior agency information security officers, • authorizing officials, • information owners, • Smart Grid information system and mission owners, • Smart Grid information system security officers, • Smart Grid information system security managers, • personnel officers, • human resource managers, • facilities managers, • training officers, • Smart Grid information system operators, • network and system administrators, • site managers, • physical security officers, and • users.	The depth attribute addresses the rigor of and level of detail in the interview process. There are three possible values for the depth attribute: (i) basic; (ii) focused; and (iii) comprehensive. • Basic interview: Interview that consists of broad-based, high-level discussions with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions. Basic interviews provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors. • Focused interview: Interview that consists of broad-based, high-level discussions and more in depth discussions in specific areas with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions and more in depth questions in specific areas where responses indicate a need for more in depth investigation. Focused interviews provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended. • Comprehensive interview: Interview that consists of broad-based, high-level discussions and more in depth, probing discussions in specific areas with individuals or groups of individuals. This type of interview is conducted using a set of generalized, high-level questions and more in depth, probing questions in specific areas where responses indicate a need for more in depth investigation. Comprehensive interviews provide a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.	The coverage attribute addresses the scope or breadth of the interview process and includes the types of individuals to be interviewed (by organizational role and associated responsibility), the number of individuals to be interviewed (by type), and specific individuals to be interviewed.46 There are three possible values for the coverage attribute: (i) basic, (ii) focused; and (iii) comprehensive. • Basic interview: Interview that uses a representative sample of individuals in key organizational roles to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors. • Focused interview: Interview that uses a representative sample of individuals in key organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended. • Comprehensive interview: Interview that uses a sufficiently large sample of individuals in key organizational roles and other specific individuals deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.

ASSESSMENT METHOD	ASSESSMENT OBJECTS	DEFINITION	SUPPLEMENTAL GUIDANCE	ATTRIBUTE: Depth	ATTRIBUTE: Coverage
Test	Mechanisms (e.g., hardware, software, firmware) Activities (e.g., system operations, administration, management; exercises)	The process of exercising one or more assessment objects under specified conditions to compare actual with expected behavior. The results are used to support the determination of security control existence, functionality, correctness, completeness, and potential for improvement over time.	Typical assessor actions may include, for example: • testing access control, identification and authentication, and audit mechanisms; • testing security configuration settings; • testing physical access control devices; conducting penetration testing of key Smart Grid information system components; • testing Smart Grid information system backup operations; • testing incident response capability; and • exercising contingency planning capability.	The depth attribute addresses the types of testing to be conducted. There are three possible values for the depth attribute: (i) basic testing; (ii) focused testing; and (iii) comprehensive testing. • Basic testing: Test methodology (also known as black box testing) that assumes no knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification for mechanisms and a high-level process description for activities. Basic testing provides a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors. • Focused testing: Test methodology (also known as gray box testing) that assumes some knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification and limited system architectural information (e.g., high-level design) for mechanisms and a high-level process description and high-level description of integration into the operational environment for activities. Focused testing provides a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended. • Comprehensive testing: Test methodology (also known as white box testing) that assumes explicit and substantial knowledge of the internal structure and implementation detail of the assessment object. This type of testing is conducted using a functional specification, extensive system architectural information (e.g., high-level design, low-level design) and implementation representation (e.g., source code, schematics) for mechanisms and a high-level process description and detailed description of integration into the operational environment for activities. Comprehensive testing provides a level of understanding of the security control necessary for determining whether the control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.	The coverage attribute addresses the scope or breadth of the testing process and includes the types of assessment objects to be tested, the number of objects to be tested (by type), and specific objects to be tested.48 There are three possible values for the coverage attribute: (i) basic; (ii) focused; and (iii) comprehensive. • Basic testing: Testing that uses a representative sample of assessment objects (by type and number within type) to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors. • Focused testing: Testing that uses a representative sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are increased grounds for confidence that the control is implemented correctly and operating as intended. • Comprehensive testing: Testing that uses a sufficiently large sample of assessment objects (by type and number within type) and other specific assessment objects deemed particularly important to achieving the assessment objective to provide a level of coverage necessary for determining whether the security control is implemented and free of obvious errors and whether there are further increased grounds for confidence that the control is implemented correctly and operating as intended on an ongoing and consistent basis, and that there is support for continuous improvement in the effectiveness of the control.